#3

Docket No.: 57454-066

PATENT

JC903 U.S. PTO
09/823996
04/03/01

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	
Tadaaki YAMAUCHI, et al.	:	
Serial No.:	:	Group Art Unit:
Filed: April 03, 2001	:	Examiner:

For: SEMICONDUCTOR MEMORY DEVICE INTERNALLY PROVIDED WITH LOGIC CIRCUIT WHICH CAN BE READILY CONTROLLED AND CONTROLLING METHOD THEREOF

CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Commissioner for Patents
Washington, DC 20231

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2000-299012,
filed September 29, 2000

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Stephen A. Becker
Registration No. 26,527

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 SAB:dtb
Date: April 3, 2001
Facsimile: (202) 756-8087

P1454-060
Yamauchi, et al.
April 3, 2001
McDermott, Will & Emery

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

jc903 U.S. PTO
09/823996

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　９月２９日

出願番号
Application Number: 特願２０００－２９９０１２

出願人
Applicant (s): 三菱電機株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年１０月２０日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０８７３５７

【書類名】　特許願
【整理番号】　527098JP01
【提出日】　平成12年 9月29日
【あて先】　特許庁長官殿
【国際特許分類】　G11C 11/34
【発明者】
【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
【氏名】　山内　忠昭
【発明者】
【住所又は居所】　東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
【氏名】　小猿　邦彦
【特許出願人】
【識別番号】　000006013
【氏名又は名称】　三菱電機株式会社
【代理人】
【識別番号】　100064746
【弁理士】
【氏名又は名称】　深見　久郎
【選任した代理人】
【識別番号】　100085132
【弁理士】
【氏名又は名称】　森田　俊雄
【選任した代理人】
【識別番号】　100091409
【弁理士】
【氏名又は名称】　伊藤　英彦

【選任した代理人】

【識別番号】　100096781

【弁理士】

【氏名又は名称】　堀井　豊

【選任した代理人】

【識別番号】　100096792

【弁理士】

【氏名又は名称】　森下　八郎

【手数料の表示】

【予納台帳番号】　008693

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　半導体記憶装置および半導体記憶装置の制御方法

【特許請求の範囲】

【請求項１】　外部から与えられる制御信号、アドレスおよびデータを受ける端子群と、

前記アドレスによって指定される領域に対して前記制御信号に応じて前記データの授受を行なうメモリセルアレイと、

前記メモリセルアレイに対して前記制御信号、前記アドレスおよび前記データが与えられるシーケンスと同じシーケンスで前記端子群に前記制御信号、前記アドレスおよび前記データが与えられた場合に、前記アドレスが所定の第１の領域を指定したときに前記制御信号、前記アドレスおよび前記データの少なくともいずれか１つに応じてデータ処理を行なうロジック回路とを備える、半導体記憶装置。

【請求項２】　前記端子群から前記制御信号、前記アドレスおよび前記データを受け、前記アドレスに応じて前記メモリセルアレイと前記ロジック回路のいずれか一方に対して、前記制御信号、前記アドレスおよび前記データの少なくともいずれか１つに応じた動作を指示するインターフェイス部をさらに備え、

前記ロジック回路は、

前記インターフェイス部からの指示内容を保持するデータ保持部と、

前記データ保持部の保持内容に応じてデータ処理を行なうデータ処理回路とを含む、請求項１に記載の半導体記憶装置。

【請求項３】　前記指示内容は、

前記データ処理回路の動作を指定するコマンドと、

前記データ処理回路が処理する入力データとを含み、

前記データ保持部は、

前記コマンドを保持する第１の保持回路と、

前記入力データを保持する第２の保持回路と、

前記入力データを前記データ処理回路がデータ処理した処理結果を保持する第３の保持回路とを含む、請求項２に記載の半導体記憶装置。

【請求項４】　前記データ保持部は、

前記データ処理回路がデータ処理を完了したか否かを示すフラグを保持する第４の保持回路をさらに含む、請求項３に記載の半導体記憶装置。

【請求項５】　前記データ処理回路は、暗号処理を行ない、

前記入力データは、

暗号の鍵データを含む、請求項３に記載の半導体記憶装置。

【請求項６】　前記指示内容は、

前記データ処理回路の複数の動作モードの指定を含み、

前記データ保持部は、

前記複数の動作モードを保持する保持回路を有し、

前記保持回路は、前記メモリアレイに一回に書込むデータ幅分のビットの容量を有し、

前記ロジック回路に対する前記複数の動作モードの指定は、前記メモリセルアレイに対する１回のデータ書込を行なうシーケンスと同じシーケンスで行なわれる、請求項２に記載の半導体記憶装置。

【請求項７】　前記インターフェイス部は、

前記制御信号に応じて書換え可能なモードレジスタを含み、

前記インターフェイス部は、前記モードレジスタの保持値に応じて前記第１の領域をアドレス空間のどこに割当てるかを決定する、請求項２に記載の半導体記憶装置。

【請求項８】　前記所定の第１の領域は、

前記メモリセルアレイのアドレス空間の一部の領域である、請求項１に記載の半導体記憶装置。

【請求項９】　前記所定の第１の領域は、

前記メモリセルアレイのアドレス空間以外の仮想的なアドレス空間の一部の領域である、請求項１に記載の半導体記憶装置。

【請求項１０】　前記ロジック回路は、仮想的なアドレス空間の一部である前記所定の第１の領域へのアクセスに応じて、前記所定の第１の領域に対応する前記メモリセルアレイのアドレス空間に格納されたデータに処理を加える、請求

項９に記載の半導体記憶装置。

【請求項１１】　外部から与えられる制御信号、アドレスおよびデータを受ける端子群と、前記アドレスによって指定される領域に対して前記制御信号に応じて前記データの授受を行なうメモリセルアレイと、前記メモリセルアレイに対して前記制御信号、前記アドレスおよび前記データが与えられるシーケンスと同じシーケンスで前記端子群に前記制御信号、前記アドレスおよび前記データが与えられた場合に、前記アドレスが所定の第１の領域を指定したときに前記制御信号、前記アドレスおよび前記データの少なくともいずれか１つに応じてデータ処理を行なうロジック回路とを備える半導体記憶装置の制御方法であって、

前記第１の領域を予約領域に指定するステップと、

前記メモリセルアレイへの書込シーケンスと同じシーケンスで前記アドレスによって前記第１の領域を指定して前記ロジック回路へのコマンドを与えるステップとを備える、半導体記憶装置の制御方法。

【請求項１２】　前記メモリセルアレイへの読出シーケンスと同じシーケンスで前記第１の領域を指定して前記ロジック回路の処理結果を読出すステップをさらに備える、請求項１１に記載の半導体記憶装置の制御方法。

【請求項１３】　前記半導体記憶装置は、前記端子群を介して、キャッシュメモリを内蔵するマイクロコンピュータと接続され、

前記第１の領域を前記キャッシュメモリを使用しない領域として指定するステップをさらに備える、請求項１１に記載の半導体記憶装置の制御方法。

【請求項１４】　外部から与えられる制御信号、アドレスおよびデータを受ける第１の端子群と、

行列状に配置される複数のメモリセルを含み、外部から与えられる選択信号に応じて活性化され、前記アドレスによって指定される領域に対して前記制御信号に応じて前記データの授受を行なうメモリと、

前記選択信号に応じて前記メモリと相補的に活性化され、前記アドレスおよび前記データの少なくともいずれか１つに応じてデータ処理を行なうロジック回路と、

前記選択信号を受ける第２の端子とを備える、半導体記憶装置。

【請求項１５】　前記メモリは、前記第１の端子群に時分割に与えられる行アドレスと列アドレスとを含む前記アドレスに応じて前記メモリセルの選択動作を行ない、

前記ロジック回路は、前記第１の端子群に一括して与えられる前記アドレスに応じて動作を行なう、請求項１４に記載の半導体記憶装置。

【請求項１６】　前記ロジック回路は、

前記行アドレスと前記列アドレスの変化を検知して動作タイミングを発生するＡＴＤ回路を含む、請求項１５に記載の半導体記憶装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、半導体記憶装置に関し、より特定的にはロジック回路を内蔵した半導体記憶装置およびその制御方法に関する。

【０００２】

【従来の技術】

図５３は、従来の、６４Ｍｂｉｔの容量を有し、ワード構成が×１６ｂｉｔであるシンクロナスダイナミックランダムアクセスメモリ（ＳＤＲＡＭ）のピン配置を示した図である。

【０００３】

図５４は、ＳＤＲＡＭの端子名と機能とを示した図である。

図５３、図５４を参照して、従来のＳＤＲＡＭは、５４ピンの端子を有するパッケージに収められており、マスタクロックが入力される端子ＣＬＫ，クロックイネーブル信号が入力される端子ＣＫＥ，チップセレクト信号が入力される端子／ＣＳ，ロウアドレスストローブ信号が入力される端子／ＲＡＳ，コラムアドレスストローブ信号が入力される端子／ＣＡＳ，ライトイネーブル信号が入力される端子／ＷＥを有している。

【０００４】

従来のＳＤＲＡＭは、さらに、データ入出力信号を授受する端子ＤＱ０～ＤＱ１５，出力ディスエーブル信号／ライトマスク信号が入出力される端子ＤＱＭ（

Ｕ／Ｌ），アドレスが入力される端子Ａ０～Ａ１１，バンクアドレスが入力される端子ＢＡ０，ＢＡ１，電源が与えられる端子ＶＤＤ，出力用電源が与えられる端子ＶＤＤＱ，接地電位が与えられる端子ＶＳＳ，出力用接地電位が与えられる端子ＶＳＳＱを有している。

【０００５】

これらの端子は、図５３に示すように、１番ピンから１３番ピンおよび４２番ピンから５４番ピンの間にデータ入出力端子および電源が配置され、１５番ピンから１９番ピンおよび３７番ピンから３９番ピンの間に制御信号およびクロック信号が配置されており、２０番ピンから３５番ピンの間にアドレス入力ピンが配置されている。このような端子配置は、ある程度汎用性を有しており、メモリを搭載するシステムに用いられる基板にもよく使われている。

【０００６】

図５５は、従来のロジック内蔵ＤＲＡＭの構成を示す図である。

図５５を参照して、チップ５０１には、ＤＲＡＭ５０４とロジック５０８が搭載されており、ＤＲＡＭへのアクセス用の制御信号／ＲＡＳ，／ＣＡＳ，…，／ＣＳや、アドレス信号ＡＤＤ．およびデータ信号ＤＡＴＡを入力する、あるいは、出力する端子が設けられている。

【０００７】

チップ５０１には、さらに、ロジック特有の制御ピンＣＴＲ０，ＣＴＲ１や、ロジックにアクセス要求をするリクエスト信号ＲＥＱを入力する端子およびロジックが処理完了を外部に知らせるためのストローブ信号ＳＴＲＢを出力するための端子を含んでいる。

【０００８】

【発明が解決しようとする課題】

従来は、ロジック５０８を制御するために、ロジック５０８のための特有なピンを設けていたため、図５３で示したような汎用的なＤＲＡＭに対してピン数が増えたり、またボード上でシステムを組むためにロジック混在ＤＲＡＭを制御するために専用のコントローラを準備する必要があった。したがって、通常のマイクロコンピュータに接続するような汎用性が失われたり、またはシステムをコン

トロールするためにマイクロコンピュータに特殊なコマンドを使う必要があった。

【０００９】

この発明の目的は、汎用的なＤＲＡＭと同様な制御方法でロジック部を制御することが可能なロジック回路を混載した半導体記憶装置を提供することである。

【００１０】

【課題を解決するための手段】

請求項１に記載の半導体記憶装置は、外部から与えられる制御信号、アドレスおよびデータを受ける端子群と、アドレスによって指定される領域に対して制御信号に応じてデータの授受を行なうメモリセルアレイと、メモリセルアレイに対して制御信号、アドレスおよびデータが与えられるシーケンスと同じシーケンスで端子群に制御信号、アドレスおよびデータが与えられた場合に、アドレスが所定の第１の領域を指定したときに制御信号、アドレスおよびデータの少なくともいずれか１つに応じてデータ処理を行なうロジック回路とを備える。

【００１１】

請求項２に記載の半導体記憶装置は、請求項１に記載の半導体記憶装置の構成に加えて、端子群から制御信号、アドレスおよびデータを受け、アドレスに応じてメモリセルアレイとロジック回路のいずれか一方に対して、制御信号、アドレスおよびデータの少なくともいずれか１つに応じた動作を指示するインターフェイス部をさらに備え、ロジック回路は、インターフェイス部からの指示内容を保持するデータ保持部と、データ保持部の保持内容に応じてデータ処理を行なうデータ処理回路とを含む。

【００１２】

請求項３に記載の半導体記憶装置は、請求項２に記載の半導体記憶装置の構成に加えて、指示内容は、データ処理回路の動作を指定するコマンドと、データ処理回路が処理する入力データとを含み、データ保持部は、コマンドを保持する第１の保持回路と、入力データを保持する第２の保持回路と、入力データをデータ処理回路がデータ処理した処理結果を保持する第３の保持回路とを含む。

【００１３】

請求項４に記載の半導体記憶装置は、請求項３に記載の半導体記憶装置の構成に加えて、データ保持部は、データ処理回路がデータ処理を完了したか否かを示すフラグを保持する第４の保持回路をさらに含む。

【００１４】

請求項５に記載の半導体記憶装置は、請求項３に記載の半導体記憶装置の構成において、データ処理回路は、暗号処理を行ない、入力データは、暗号の鍵データを含む。

【００１５】

請求項６に記載の半導体記憶装置は、請求項２に記載の半導体記憶装置の構成において、指示内容は、データ処理回路の複数の動作モードの指定を含み、データ保持部は、複数の動作モードを保持する保持回路を有し、保持回路は、メモリアレイに一回に書込むデータ幅分のビットの容量を有し、ロジック回路に対する複数の動作モードの指定は、メモリセルアレイに対する１回のデータ書込を行なうシーケンスと同じシーケンスで行なわれる。

【００１６】

請求項７に記載の半導体記憶装置は、請求項２に記載の半導体記憶装置の構成に加えて、インターフェイス部は、制御信号に応じて書換え可能なモードレジスタを含み、インターフェイス部は、モードレジスタの保持値に応じて第１の領域をアドレス空間のどこに割当てるかを決定する。

【００１７】

請求項８に記載の半導体記憶装置は、請求項１に記載の半導体記憶装置の構成において、所定の第１の領域は、メモリセルアレイのアドレス空間の一部の領域である。

【００１８】

請求項９に記載の半導体記憶装置は、請求項１に記載の半導体記憶装置の構成において、所定の第１の領域は、メモリセルアレイのアドレス空間以外の仮想的なアドレス空間の一部の領域である。

【００１９】

請求項１０に記載の半導体記憶装置は、請求項９に記載の半導体記憶装置の構

成において、ロジック回路は、仮想的なアドレス空間の一部である所定の第１の領域へのアクセスに応じて、所定の第１の領域に対応するメモリセルアレイのアドレス空間に格納されたデータに処理を加える。

【００２０】

請求項１１に記載の半導体記憶装置の制御方法は、外部から与えられる制御信号、アドレスおよびデータを受ける端子群と、アドレスによって指定される領域に対して制御信号に応じてデータの授受を行なうメモリセルアレイと、メモリセルアレイに対して制御信号、アドレスおよびデータが与えられるシーケンスと同じシーケンスで端子群に制御信号、アドレスおよびデータが与えられた場合に、アドレスが所定の第１の領域を指定したときに制御信号、アドレスおよびデータの少なくともいずれか１つに応じてデータ処理を行なうロジック回路とを備える半導体記憶装置の制御方法であって、第１の領域を予約領域に指定するステップと、メモリセルアレイへの書込シーケンスと同じシーケンスでアドレスによって第１の領域を指定してロジック回路へのコマンドを与えるステップとを備える。

【００２１】

請求項１２に記載の半導体記憶装置の制御方法は、請求項１１に記載の半導体記憶装置の制御方法の構成に加えて、メモリセルアレイへの読出シーケンスと同じシーケンスで第１の領域を指定してロジック回路の処理結果を読出すステップをさらに備える。

【００２２】

請求項１３に記載の半導体記憶装置の制御方法は、請求項１１に記載の半導体記憶装置の制御方法の構成に加えて、半導体記憶装置は、端子群を介して、キャッシュメモリを内蔵するマイクロコンピュータと接続され、第１の領域をキャッシュメモリを使用しない領域として指定するステップをさらに備える。

【００２３】

請求項１４に記載の半導体記憶装置は、外部から与えられる制御信号、アドレスおよびデータを受ける第１の端子群と、行列状に配置される複数のメモリセルを含み、外部から与えられる選択信号に応じて活性化され、アドレスによって指定される領域に対して制御信号に応じてデータの授受を行なうメモリと、選択信

号に応じてメモリと相補的に活性化され、アドレスおよびデータの少なくともいずれか１つに応じてデータ処理を行なうロジック回路と、選択信号を受ける第２の端子とを備える。

【００２４】

請求項１５に記載の半導体記憶装置は、請求項１４に記載の半導体記憶装置の構成において、メモリは、第１の端子群に時分割に与えられる行アドレスと列アドレスとを含むアドレスに応じてメモリセルの選択動作を行ない、ロジック回路は、第１の端子群に一括して与えられるアドレスに応じて動作を行なう。

【００２５】

請求項１６に記載の半導体記憶装置は、請求項１５に記載の半導体記憶装置の構成に加えて、ロジック回路は、行アドレスと列アドレスの変化を検知して動作タイミングを発生するＡＴＤ回路を含む。

【００２６】

【発明の実施の形態】

以下において、本発明の実施の形態について図面を参照して詳しく説明する。なお、図中同一符号は同一または相当部分を示す。

【００２７】

［実施の形態１］

図１は、本発明の実施の形態１の半導体記憶装置１の構成を示したブロック図である。

【００２８】

図１を参照して、半導体記憶装置１は、制御信号／ＲＡＳ，／ＣＡＳ，…，／ＣＳ，／ＷＥなどの制御信号を受ける端子とアドレス信号ＡＤＤを受ける端子とデータ信号ＤＡＴＡを受ける端子と、制御信号／ＲＡＳ，／ＣＡＳ，…，／ＣＳ，／ＷＥ、アドレス信号ＡＤＤ．およびデータ信号ＤＡＴＡに応じて内部に制御信号を出力するインターフェイス部２と、インターフェイス部２の出力を受けて動作をするＤＲＡＭ４と、インターフェイス部２から与えられるデータやコマンドとを保持するレジスタ６と、レジスタ６およびインターフェイス部２からの出力に応じて信号処理などの動作を行なうロジック回路８とを含む。

【００２９】

チップ１の端子は、汎用ＤＲＡＭで用いられている端子のみである。したがって、汎用ＤＲＡＭチップを収めているのと同じパッケージを用いることができる。たとえば図５３に示したようなピン配置を有するパッケージである。

【００３０】

そのため、本発明の半導体記憶装置１を既存のアプリケーションで用いる場合に、既存の汎用ＤＲＡＭと入換えるだけであるので、ボードの再設計や専用の制御ＬＳＩを開発する必要がない。すなわち、汎用ＤＲＡＭとピンコンパチブルであるため、ソフトウェアの変更だけで、新たな機能を追加することができる。たとえば新たな機能としては、画像の高速処理用の回路や、暗号処理などのマイクロコンピュータでは時間がかかってしまう処理を行なうロジック回路の追加が考えられる。また、汎用ＤＲＡＭを収めているパッケージに数本の未使用の端子、たとえば図５３における３６番ピンや４０番ピンのようなＮＣ（ノンコネクション）ピンを用いて制御信号を入力するようにしてもよい。

【００３１】

次に、具体的な制御方法を説明する。搭載されるロジック回路の制御には、いわゆるメモリマップドＩＯ方式を適用する。

【００３２】

図２は、実施の形態１のロジック内蔵半導体記憶装置のメモリマップの例を示した図である。

【００３３】

図２を参照して、チップに搭載されるＤＲＡＭの容量を６４Ｍｂｉｔとし、ワード構成を×１６とする。ＤＲＡＭのアドレスは、Ｘアドレスが Ｘ０～Ｘ１３，Ｙアドレスが Ｙ０～Ｙ７である。よって、８ＭＢｙｔｅを制御するメモリアドレスは０ｈ～３ＦＦＦＦＦｈである。

【００３４】

汎用のＤＲＡＭでは、このアドレス空間すべてにデータをライトしてリードできる。このようなデータをライトしてリードできる空間をＤＲＡＭ空間と呼ぶことにする。本発明では、ある特定の領域を搭載するロジック回路のためのロジッ

ク制御領域に割当てる。たとえばアドレスの０ｈ～１Ｆｈの空間をロジック制御領域に割当てる。ロジック制御領域の容量は、たとえば、２５６×２Ｂｙｔｅの５１２Ｂｙｔｅである。このアドレス空間に書込むデータによってロジックを制御するコマンドやモードを選択することができる。

【００３５】

図２では、最下位アドレスに領域を確保したが、最上位側（３ＦＦＦＦＦｈ～３ＦＦＥ０ｈ）にロジック制御領域を割当ててもよい。搭載するＤＲＡＭとしてＳＤＲＡＭを想定した場合には、モードレジスタセット時にアドレスを割当てる領域を選択することができるようにしてもよい。また、モードレジスタセット時にロジック制御領域を割当てなければ、通常の６４ＭｂｉｔのＳＤＲＡＭとして使用することもできる。

【００３６】

図３は、外部から入力される信号がロジック回路へ伝達される様子を説明するための図である。

【００３７】

図３を参照して、インターフェイス部２は、制御信号／ＲＡＳ，／ＣＡＳ，…，／ＣＳ，／ＷＥ、アドレス信号ＡＤＤ．およびデータ信号ＤＡＴＡを受けるバッファ３と、バッファ３の出力を受けてデコードするデコード回路５とを含んでおり、デコード回路５の出力に応じてレジスタ６はモードやコマンドなどの情報を保持し、これらの保持した情報に応じてロジック回路８が制御される。

【００３８】

デコード回路５は、アドレス信号ＡＤＤとデータ信号ＤＡＴＡをデコードするが、アドレス信号によって指定されるロジック制御領域に書込まれたデータをそのままレジスタ６に保存する場合もある。レジスタが、ＳＲＡＭ（スタティックランダムアクセスメモリ）などで構成されている場合には、アドレス信号ＡＤＤに応じて指定されるＳＲＡＭの領域にデータが保持される場合もある。また、レジスタ６の代わりに保持回路としてＤＲＡＭの一部の領域を用い、その領域にロジック回路制御用のデータを保持させてもよい。

【００３９】

図４は、実施の形態１の半導体記憶装置の標準的なタイミングを説明するための波形図である。

【００４０】

図４においては、データ入出力端子から入力および出力が可能なＳＤＲＡＭにおいて、連続して８つのデータを書込みまたは読出す動作を示す。連続して読出されるデータのビット数はバースト長と呼ばれ、ＳＤＲＡＭでは通常モードレジスタによって変更することが可能である。

【００４１】

図４を参照して、時刻ｔ１において、外部からのクロック信号ｅｘｔ．ＣＬＫ（たとえばシステムクロック）の立上がりエッジで外部からの制御信号（ロウアドレスストローブ信号／ＲＡＳ、コラムアドレスストローブ信号／ＣＡＳ、アドレス信号ＡＤＤなど）が取込まれる。ロウアドレスストローブ信号／ＲＡＳが活性状態のＬレベルにあり、コラムアドレスストローブ信号／ＣＡＳおよびライトイネーブル信号／ＷＥはＨレベルにあるため、ロウアクティブコマンドＡＣＴが入力されたことになる。このときのアドレス信号ＡＤＤはロウアドレスＸａとして取込まれる。

【００４２】

時刻ｔ２において、コラムアドレスストローブ信号／ＣＡＳが活性状態のＬレベルとなり、クロック信号ｅｘｔ．ＣＬＫの立上がりに同期して内部に取込まれる。コラムアドレスストローブ信号／ＣＡＳがＬレベルで、ロウアドレスストローブ信号／ＲＡＳおよびライトイネーブル信号／ＷＥがＨレベルという制御信号の組み合わせは、リードコマンドＲＥＡＤである。このときのアドレス信号ＡＤＤはコラムアドレスＹとして取込まれる。

【００４３】

アドレスで指定された領域が、図２のＤＲＡＭ空間である場合には、この取込まれたロウアドレスＸａおよびコラムアドレスＹｂに従って図１のＤＲＡＭ４内において行および列の選択動作が実施される。

【００４４】

ロウアドレスＸａおよびコラムアドレスＹｂが図２のロジック指定領域のアド

レスである場合には、選択されるのは、図１のＤＲＡＭ４の行および列ではなく、レジスタ６の所定の領域である。たとえば、この所定の領域には、ロジック８の動作状態を示すフラグや、ロジック８の演算結果が格納されている。

【００４５】

Ｄ／Ｑは、データ入出力端子から入出力されるデータ信号ＤＡＴＡを示す。ロウアドレスストローブ信号／ＲＡＳがＬレベルに立下がってから所定のクロック周期（図４においては６クロックサイクル）が経過した後時刻ｔ３において最初のデータｑ０が出力され、データｑ０に引き続きデータｑ１～ｑ７が連続して出力される。このデータの出力はクロック信号ｅｘｔ．ＣＬＫの立下がりに応答して出力される。

【００４６】

この出力されたデータは、ＤＲＡＭ４に保持されていたデータ、または、レジスタ６の内容である。レジスタ６の内容は、たとえば、ロジック８の動作状態を示すフラグや、ロジック８の演算結果である。

【００４７】

時刻ｔ４以降は書込動作を示す。時刻ｔ４において、ロウアクティブコマンドＡＣＴが入力され、ロウアドレスＸｃが取込まれる。時刻ｔ５において、コラムアドレスストローブ信号／ＣＡＳおよびライトイネーブル信号／ＷＥがともに活性状態のＬレベルであり、かつ、ロウアドレスストローブ信号／ＲＡＳがＨレベルの組合せ、すなわち、ライトコマンドＷＲＩＴＥが与えられると、そのときのクロック信号ｅｘｔ．ＣＬＫの立上がりエッジにおいてコラムアドレスＹｄが取込まれるとともに、そのときに与えられていたデータｄ０が最初の書込データとして取込まれる。

【００４８】

アドレスで指定された領域が、図２のＤＲＡＭ空間である場合には、ロウアドレスストローブ信号／ＲＡＳおよびコラムアドレスストローブ信号／ＣＡＳの立下がりに応答して、ＳＤＲＡＭ内部においては行および列選択動作が実施される。以降クロック信号ｅｘｔ．ＣＬＫに同期して順次入力データｄ１～ｄ７が取込まれ、対応するメモリセルに書込まれる。

【００４９】

ロウアドレスＸｃおよびコラムアドレスＹｄで指定される領域が、図２のロジック指定領域である場合には、選択されるのは、図１のＤＲＡＭ４の行および列ではなく、レジスタ６の所定の領域である。この場合は、入力データｄ１～ｄ７は、レジスタ６の所定の領域に書込むデータである。たとえば、与えるデータは、ロジック８が処理する画像データ、暗号データ等の処理データや、リセット、処理開始等の動作を指定するコマンドデータである。

【００５０】

［実施の形態１の変形例］

図５は、実施の形態１の変形例であるロジック内蔵ＤＲＡＭ１０の構成を示すブロック図である。

【００５１】

図５を参照して、ロジック内蔵ＤＲＡＭ１０は、制御信号／ＲＡＳ，／ＣＡＳ，…，／ＣＳ、アドレス信号ＡＤＤ、データ信号ＤＡＴＡを受けるインターフェイス１２と、インターフェイス部１２の出力に応じて動作するＤＲＡＭ４と、インターフェイス部１２の出力に応じて制御用データを保持するレジスタ１４，１６と、レジスタ１４，１６にそれぞれ保持される制御用データに応じて動作するロジック回路１８，２０を有する。

【００５２】

図６は、図５に示したロジック内蔵ＤＲＡＭ１０のメモリマップを示した図である。

【００５３】

図６を参照して６４Ｍｂａｔのアドレス空間０ｈ～３ＦＦＦＦＦｈのうちアドレス０ｈ～１Ｆｈはロジック回路１８に対する制御コマンドやデータを書込むロジック制御領域であり、アドレス２０ｈ～２Ｆｈは、ロジック回路２０に対するコマンドやデータを書込むロジック制御領域である。

【００５４】

このように、メモリマップドＩＯ空間を、複数個に分割し、搭載する複数個のロジック回路を制御することが可能となる。

【００５５】

「実施の形態２］

図７は、実施の形態２のロジック内蔵ＤＲＡＭ３０の構成を示すブロック図である。

【００５６】

図７を参照して、ロジック内蔵ＤＲＡＭ３０は、ＳＤＲＡＭ部３２と、ロジック部３４とを含む。

【００５７】

ＳＤＲＡＭ部３２は、外部からの信号を受けてそれに応じた制御信号を出力するインターフェイス部３６と、インターフェイス部３６からの出力に応じてデータの保持を行なうＤＲＡＭコア３８とを含む。インターフェイス部３６は、制御信号／ＣＳ，／ＲＡＳ，／ＣＡＳ，／ＷＥおよびＤＱＭを受ける制御信号入力回路４０と、クロック信号ＣＬＫおよびクロックイネーブル信号ＣＫＥを受けて内部クロックを発生するクロックバッファ４４と、クロックバッファ４４の出力に同期してアドレス信号Ａ０～Ａｎを取込むアドレスバッファ４６と、内部クロックに同期してデータ信号ＤＱ０～ＤＱｎの入出力を行なう入出力回路５２とを含む。

【００５８】

インターフェイス部３６は、さらに、制御信号入力回路４０の出力に応じコマンド信号ＡＣＴ，ＰＲＥなどを出力する制御回路４２と、制御回路４２の出力に応じてアドレスバッファ４６の出力をＸアドレス，Ｙアドレスとしてマルチプレクスするマルチプレクサ４８とを含む。

【００５９】

マルチプレクサ４８は、モードレジスタセット（ＭＲＳ）コマンドに応じてアドレス信号Ａ０～Ａｍのいずれかの信号ビットに応じて設定可能なモードレジスタ５０を含んでいる。

【００６０】

ＤＲＡＭコア３８は、行列状にメモリセルが配置されるメモリセルアレイ５４と、マルチプレクサ４８から与えられるロウアドレスに応じてメモリセルアレイ

５４の行選択を行なうロウデコーダ５６と、マルチプレクサ４８から与えられるコラムアドレスに応じてメモリセルアレイ５４の列選択を行なうロウデコーダ５６と、選択されたメモリセルからデータを読出し、かつ、選択されたメモリセルに対してデータの書込みを行なうセンスアンプドライバ&ライトドライバ６０とを含む。

【００６１】

ロジック部３４は、暗号演算ロジック７４と、インターフェイス部３６の出力に応じて暗号演算ロジック７４の制御をするためのモード情報や暗号演算ロジックに入力するデータおよび暗号演算ロジックの演算結果を保持するレジスタ部７２とを含む。

【００６２】

レジスタ部７２は、アドレス信号Ａ０～Ａｍによって指定される領域が所定値の場合に活性化され、入出力回路５２を介して外部から入力されるデータ信号を取込むためのセレクタ７６と、セレクタ７６を介して外部から与えられたデータを書込む制御レジスタ７８，モードレジスタ８０およびデータレジスタ８４と、暗号演算ロジックから出力されるデータを保持してその保持データをセレクタ７６，入出力回路５２を介して外部にデータ信号ＤＱ０～ＤＱｎとして読出すためのステータスレジスタ８２、データレジスタ８６とを含む。

【００６３】

図８は、実施の形態２のロジック内蔵ＤＲＡＭに適用されるシステムのメモリマップを示した図である。

【００６４】

図８を参照して、システムメモリマップ中の外部ＲＡＭ領域がロジック内蔵ＤＲＡＭに対応する。ロジック内蔵ＤＲＡＭは、その領域がロジック制御領域とＤＲＡＭ領域に分割されており、ロジック制御領域へのアクセスによって内蔵する暗号ロジックを制御する。このロジック制御領域に対応するシステムメモリマップ上の領域はシステム予約領域とし、ＣＰＵのキャッシュおよびMMU（メモリマネージメントユニット）を使用する場合には、キャッシュ不可能領域としておく。また、オペレーティングシステムがこの領域にロードされないように、予め

システムのファームウェアで制御する。さらに、アプリケーションプログラムもこの領域を使用禁止とする。

【００６５】

このロジック制御領域は、たとえば、ＤＲＡＭのロウアドレスＸ＝３ＦＦＦｈ，コラムアドレスＹ＝０Ｈ～ＦＦｈに割当てる。

【００６６】

図７の制御レジスタ７８はＸ＝３ＦＦＦｈ，Ｙ＝００ｈに割当てられる。モードレジスタ８０は、Ｈ＝３ＦＦＦｈ，Ｙ＝０１ｈに割当てられる。ステータスレジスタ８２は、アドレスＸ＝３ＦＦＦｈ，Ｙ＝０２ｈに割当てられる。第１のデータレジスタ８４は、アドレスＸ＝３ＦＦＦｈ，Ｙ＝０３ｈに割当てられ、第２のデータレジスタ８６は、アドレスＸ＝３ＦＦＦｈ，Ｙ＝０４ｈに割当てられる。

【００６７】

この例では、Ｘ＝３ＦＦＦｈのページ（Ｙ＝００ｈ～ＦＦｈ）を制御コマンド領域に割当てている。したがって、図７の構成でＡＣＴコマンド入力時に、Ｘ＝３ＦＦＦｈが入力された時点で、レジスタ部７２にアクセスできるようにマルチプレクサを制御しておく。さらに、レジスタのイネーブル信号やレジスタを制御しているクロックも動作させておく。このようにすれば、制御コマンドを入力期間中以外でレジスタ部７２で消費する電力を抑えることができる。また、Ｘ＝３ＦＦＦｈのページにリード、ライトコマンドが入っても既にレジスタ部７２が活性化されているので、レジスタへのアクセスが遅延されることはない。

【００６８】

図７の、暗号演算ロジック７４は、ネットワーク上のセキュリティ確保のために使われている主要な暗号方式のアクセラレータを内蔵している。この暗号演算ロジック７４は、電子認証で用いられる公開鍵方式と認証後のデータ送受信で用いられる秘密鍵暗号方式の機能をサポートしている。暗号専用のロジック回路で処理するので、処理を汎用のＣＰＵで処理するよりも低消費電力で高速に処理を行なうことができ、たとえば電池駆動のシステム等に適している。

【００６９】

図９は、図７の暗号演算ロジック７４がサポートする暗号方式を示した図である。

【００７０】

図９を参照して、暗号演算ロジック７４は、公開鍵暗号方式としてＲＳＡをサポートし、秘密鍵暗号方式としてＤＥＳ方式とＴｒｉｐｌｅ－ＤＥＳ方式とをサポートする。さらに、秘密鍵暗号方式では、主要なブロック暗号化モードであるＥＣＢ（Electric Code Book），ＣＢＣ（Cipher Block Chaining），ＯＦＢ（Output Feed Back），ＣＦＢ（Cipher Feed Back）の各モードをサポートしている。暗号演算ロジック７４は、アプリケーションの適合性を高めるため、暗号化においてクリティカルな処理が割当てられており、その他はロジック内蔵ＤＲＡＭ３０を制御するマイクロコンピュータ側でソフトウェア処理することになる。そして最大の特徴は、汎用のＳＤＲＡＭとピンコンパチブルで暗号制御が実現できることである。

【００７１】

次に、図８に示したロジック制御領域の各レジスタにどのような割当がされているかを説明する。

【００７２】

図１０～図１８は、レジスタに割当てられるデータを説明するための図である。

【００７３】

図７、図１０を参照して、制御レジスタ７８は、Ｙアドレスが０ｈのＤ０～Ｄ１５の１６ビットが割当てられている。そして、ビットＤ０に１を書込むことにより暗号機能がリセットされる。すなわち、暗号演算ロジック７４に所定時間のリセットパルスを与える処理が実行される。また、ビットＤ１が１である場合には、暗号演算ロジック７４が暗号処理中であることを示す。したがって、外部から暗号演算ロジックにアクセスする場合には、ビットＤ１に示されるフラグが０であることを確認してからアクセスしなければならない。

【００７４】

この制御レジスタ７８は、公開鍵と秘密鍵の両方式共通に用いられる。

次に秘密鍵方式の制御に用いられるいくつかのレジスタの例について説明する。

【００７５】

図７，図１１を参照して、Ｙ＝１ｈのアドレスに対しては、モードレジスタ８０が割当てられており、この１６ビットのうちビットＤ１，Ｄ０は、暗号方式選択に使用される。この２つのビットが“０１”であれば暗号方式はＤＥＳである“１０”であれば暗号方式はトリプルＤＥＳである。“００”であれば暗号方式はホールドされる。

【００７６】

ビットＤ５～Ｄ２は、ブロック暗号化モード選択に使用される。このビットが“０００１”であればブロック暗号化モードはＥＣＢが指定される。また“００１０”の場合はブロック暗号化モードはＣＢＣが指定される。“０１００”の場合には暗号モードはＯＦＢが指定される。これらのビットが“１０００”の場合にはブロック暗号化モードはＣＦＢ６４に指定される。またこれらのビットが“００００”の場合はブロック暗号化モードはホールドされる。

【００７７】

ビットＤ８～Ｄ６は暗号処理の単位量を指定するデータ処理モードの選択に使用される。これらのビットが“００１”の場合には処理を８Ｂｙｔｅ単位で行なうノーマルモードが指定され、“０１０”の場合はブロック長を指定したブロック単位で処理を行なうブロックモードが指定され、“１００”の場合にはバッファに蓄積した情報を単位として一括処理するバッファモードが指定され、“０００”の場合にはデータ処理モードはホールドされる。

【００７８】

このように、Ｙ＝１ｈの１アドレス２Ｂｙｔｅのデータの１６ビットを複数のモード指定に割当てることができるので、２の１６乗の組合せを有効に使用すれば、指定するモードが複数ある場合であっても１回のアクセスで動作モードの指定を完了することができる。

【００７９】

図７、図１２を参照して、アドレスＹ＝０２ｈにはステータスレジスタ８２が

割当てられている。ステータスレジスタのビットＤ１，Ｄ０が“０１”であるときは暗号化を示し、“１０”であるときは復号化を示し、“００”であるときはホールドを示す。ビットＤ５，Ｄ４が“０１”であるときには、平文または暗号文の入力スタートを示しており、“１０”であるときには入力ストップを示し、“００”であるときはホールドを示す。

【００８０】

ビットＤ９～Ｄ６は、ＯＦＢ，ＣＦＢの１ブロック中のテキスト長を表わす。

図７、図１３を参照して、Ｙアドレス３ｈ～６ｈは６４ビットのＤＥＳの鍵などが格納される領域である。

【００８１】

図７、図１４を参照して、第１のデータレジスタ８６は、Ｔｒｉｐｌｅ－ＤＥＳに使用される鍵を格納する領域である。アドレスＹ＝７ｈ～Ａｈの領域が相当する。

【００８２】

データレジスタ８４，８６は、ともに外部からは１本のレジスタに見えるが、実際には複数のレジスタで構成されており、一種のファーストインファーストアウト（ＦＩＦＯ）メモリである。

【００８３】

その他には、図７には図示されていないが図１５に示すような初期ベクトルを設定するレジスタ、図１６に示すようなブロック長の指定をするレジスタ、図１７に示すようなバッファ本数を指定するレジスタ、図１８に示すようなバッファＩＤを示すようなレジスタなどがある。

【００８４】

なお、公開鍵方式、たとえばＲＳＡ暗号処理を行なうために、Ｙ＝１２ｈ～１Ｆｈの領域は予約領域とされている。公開鍵方式の場合には、暗号処理結果が内蔵のレジスタに保持されるため、暗号処理中であってもＤＲＡＭ領域にアクセスすることができる。

【００８５】

ＳＤＲＡＭに対するＡＣＴコマンドで読込まれるロウアドレスＸが３ＦＦＦｈ

の場合に、マルチプレクサ４８がこれを検出しセレクタ７６を活性化する。そして、リードコマンドまたはライトコマンドでコラムアドレスＹが入力されることによりいずれのレジスタにアクセスするかが選択される。そして入出力回路５２を介して外部から入力されるデータがレジスタに書込まれる。

【００８６】

実施の形態２の場合には、ロジック制御領域として確保したアドレス領域は、３ＦＦＦ００ｈ～３ＦＦＦＦＦｈであったが、モードレジスタセット命令でセットできる図７におけるレジスタ５０の保持内容に応じて、マルチプレクサにおいて割当てアドレスを変更できるようにすることにより、さまざまなマイクロコンピュータシステムに本発明のロジック内蔵ＤＲＡＭを搭載することが可能となる。モードレジスタセット命令でアドレスを割当てない場合には、本発明のロジック内蔵ＤＲＡＭは通常の６４ＭｂｉｔのＳＤＲＡＭとして使用可能である。通常のＳＤＲＡＭとして使用する用途のために、モードレジスタに内部搭載ロジックを使用するか否かを指定するビットを設けてもよい。

【００８７】

［実施の形態３］

図１９は、本発明のロジック内蔵ＤＲＡＭ９２とマイクロコンピュータ９０とが接続される様子を示した図である。

【００８８】

マイクロコンピュータ９０には、ＣＰＵコア９４と、キャッシュメモリ９６と、メモリコントローラ９８および外部バスインターフェイス回路１００が含まれており、これらは内部バス１０２によって接続されている。外部バスインターフェイス回路１００は、ＣＰＵコア９４からの指令に応じてロジック内蔵ＤＲＡＭに対して制御信号およびアドレス信号およびデータを出力する。したがって、外部バスインターフェイス回路１００とロジック内蔵ＤＲＡＭ９２とは制御信号／ＲＡＳ，／ＣＡＳ，…，／ＣＳなどの制御信号を伝達する制御信号バスと、アドレス信号ＡＤＤ．を伝達するアドレスバスとデータＤＡＴＡを伝達するデータバスとによって接続されている。

【００８９】

このようなシステムにおいてロジック内蔵ＤＲＡＭ９２を制御するためには、マイクロコンピュータ９０上で走るソフトウェアで留意しなければならない事項がある。

【００９０】

図２０は、ロジック内蔵ＤＲＡＭの制御を説明するためのフローチャートである。

【００９１】

図２０を参照して、まず最初にステップＳ１において、ロジック制御領域となるアドレスを予約領域に指定する。つまり、ロジック回路に対するコマンド制御用のアドレス空間上にプログラムが割当てられないようにする。割当てない方法としては、たとえば、ＯＳ（オペレーションシステム）の機能を用いてロジック制御領域を予約領域にする方法がある。

【００９２】

メモリー管理、割り込み管理、プロセス間通信といったシステムの基本的な制御を行う、ＯＳにおける中核部分であるカーネル自体がロジック制御領域に割当てられないように、ＯＳの立上がり時点にも注意を要する。したがって、カーネル自体がロジック制御領域に割当てられないように注意して、予約領域をＯＳ側で指定しておく。

【００９３】

次に、ステップＳ２において、データキャッシュありのシステムにおいては、ロジック制御領域をキャッシュ不可能領域にしている。

【００９４】

すなわち、図１９におけるＣＰＵコア９４からロジック内蔵ＤＲＡＭ９２に対して所定のアドレス空間を指定してコマンドに相当するデータを内部バス１０２に送った場合であっても、キャッシュメモリ９６が動作すると、そのコマンドに相当するデータはキャッシュメモリ９６に書込まれてしまい、ロジック内蔵ＤＲＡＭ９２には伝達されない場合があり得る。すると、ロジック内蔵ＤＲＡＭ９２に搭載しているロジック回路は、そのコマンドに応じて動作できなくなる。したがって、ロジック制御領域がキャッシュされないように設定する必要がある。大

抵のマイクロコンピュータでは、一部のアドレス空間をアンキャッシャブル領域に指定する制御が可能である。

【００９５】

また、メモリマネージメントユニット機能を有している場合には、仮想アドレス空間がロジック制御領域で用いられないように設定する。

【００９６】

このように、キャッシュメモリがあるようなシステムでは、システムの初期設定において、ロジック内蔵ＤＲＡＭのロジック制御領域に対しては、キャッシュメモリを使用しないようにし、必ずアクセスされるようにする。

【００９７】

次に、ステップＳ３において、割当てた領域にノーマルライトすることによってロジック制御のためのコマンドを入力し、ステップＳ４においてノーマルリードによりロジックの処理状況のチェックや処理結果の読出を行なうことができる。さらに、ステップＳ５において処理がまだ終了していなければ、ステップＳ３，Ｓ４を繰返すことになる。具体的には、図１０で説明したように、アドレスＹ＝０ｈのビットＤ１に書込まれているフラグをチェックすることにより、処理状況を判断することができる。このフラグをチェックして、処理の完了を確認してからマイクロコンピュータは演算結果をアクセスするなど次の動作を始めることができる。

【００９８】

したがって、本発明によれば、従来では処理の終了を専用のピンで受け手側に伝えていたのに対しＳＤＲＡＭに通常のノーマルリードを行なうことによりフラグ状態をチェックすることが可能となる。

【００９９】

［実施の形態４］

実施の形態１～実施の形態３で示した例は、チップに搭載するＤＲＡＭメモリの一部の空間をつぶしてコマンド制御用の空間を割当てていた。したがって、割当てた部分だけはマイクロコンピュータシステムのメインメモリとしては使えなかった。

【０１００】

実施の形態４では、ゴースト空間を制御用に割当てる。

図２１は、実施の形態４において割当てたメモリマップを示した図である。

【０１０１】

図２１を参照して、搭載するＤＲＡＭを、６４Ｍｂｉｔの容量でワード構成が×１６のＳＤＲＡＭであるとすると、Ｘアドレスは Ｘ０～Ｘ１３、Ｙアドレスは Ｙ０～Ｙ７であった。Ｘアドレスを１端子追加し、Ｘ１４＝“０”の領域を実メモリ空間とし、Ｘ１４＝“１”の領域をゴースト空間とする。メモリが存在しないこのダミーのゴースト空間の一部をロジック制御領域に割当てる。この空間には必ず直接アクセスがされるように実施の形態３で示したような工夫をしておく。

【０１０２】

Ｘ１４を与えるための端子が１端子増加することになるが、パッケージで未使用端子がある場合にはそれを割当てればよい。たとえば図５３の４０番ピンや３６番ピンなどのＮＣ端子を割当てればよい。図２１ではＸ１４のアドレスを追加した場合を示したが、Ｙアドレスを１ビット追加してもよい。すなわちＹ８＝０の領域をＤＲＡＭ空間とし、Ｙ８＝１の領域をゴースト空間とすることもできる。ＤＲＡＭではＸアドレスとＹアドレスとは、通常はマルチプレクスされており、Ｘアドレスのほうがビットが多いので、Ｙアドレスを追加する場合には、使用する端子の追加は必要ない。

【０１０３】

以上は、ゴースト空間の一部にロジック制御領域を割当てた場合を示したが、ゴースト空間に対してリードすると、それに対応する実空間のアドレスに格納されているデータに演算が加えられて出力されたり、そのアドレスのデータが書き直される場合も考えられる。すなわち、Ｘ１４＝１としてアクセスすると、指定したアドレスのＸ１４＝０とした実空間のアドレスに保持されているデータに何らかの処理を加えるようにしてもよい。この場合においても、Ｘ１４のアドレスを拡張する代わりにＹ８のアドレスを拡張してもよく、また、Ｘ１４が１の場合にゴースト空間としたが、Ｘ１４＝０の場合をゴースト空間とし、Ｘ１４＝１の

場合を実メモリ空間としてもよい。Ｙ８のアドレスを拡張する場合もＹ８＝０の場合をゴースト空間とし、Ｙ８＝１の場合を実メモリ空間としてもよい。

【０１０４】

［実施の形態５］

図２２は、実施の形態５のロジック内蔵ＤＲＡＭ１１１の構成を示した図である。

【０１０５】

図２２を参照して、ロジック内蔵ＤＲＡＭ１１１には、通常のＤＲＡＭ１１４を制御するためのアドレスＡＤＤ．、データＤＱおよびクロック信号ＣＬＫや制御信号／ＲＡＳ，／ＣＡＳ，…，／ＣＳ，／ＷＥを制御するための端子に加えて、信号ＷＥ＿Ｌ，ＡＤＤ＿Ｌを与えるための端子が設けられている。

【０１０６】

ロジック内蔵ＤＲＡＭ１１１は、さらに、通常のＤＲＡＭ１１４と、所定の制御信号を保持するためのレジスタ１１６と、レジスタ１１６の保持情報に応じて動作するロジック回路１１８とを含む。

【０１０７】

すなわち、制御専用の端子を最小限付け加えることによって制御空間を自由に設定することができる。図２２では、追加した制御端子は、制御信号ＷＥ＿Ｌ，ＡＤＤ＿Ｌが入力される端子である。追加する端子は、図５３で示した３６ピンや４０ピンのようなＮＣピンに割当てればよい。

【０１０８】

制御信号ＡＤＤ＿ＬがＬレベルの場合にＤＲＡＭアクセスモードにされ、制御信号ＡＤＤ＿ＬがＬレベルからＨレベルになると、ＤＲＡＭ１１４は非活性化され代わりにレジスタ１１６に信号が入力可能となりロジック１１８が動作するモードとなる。

【０１０９】

図２３は、実施の形態５におけるマイクロコンピュータシステムのメモリマップを示した図である。

【０１１０】

図２３を参照して、０ｈ～３ＦＦＦＦＦｈがＤＲＡＭ空間に割当てられる。Ｘアドレスが Ｘ０～Ｘ１３の１４ビット、Ｙアドレスが Ｙ０～Ｙ７の８ビットであり、マイクロコンピュータシステムにおいてＤＲＡＭ空間を指定するアドレスビットとしては、あわせてＡ０～Ａ２１までが用いられる。

【０１１１】

そして、たとえば、制御信号ＡＤＤ＿Ｌが入力される端子をマイクロコンピュータシステムのアドレスビットＡ２３と接続した場合には、ロジック制御領域は、８０００００ｈ～８０３ＦＦＦｈを割当てることができる。つまり、アドレスビットＡ２３＝“１”とし、アドレスピンマルチプレクスを使用しないときに、アドレスを入力する最大数の端子からＤＲＡＭのアドレスとして指定することができる範囲すなわち、Ｘアドレスとして指定可能な範囲と同じ０ｈ～３ＦＦＦｈがロジック制御領域として割当可能な範囲である。実際に使用する際には、ロジック制御領域の上限は必要に応じて設定すればよい。

【０１１２】

ただし、マイクロコンピュータが、アドレスビットＡ２３＝“１”である他のアドレス領域を使用する可能性がある場合には、ロジック制御領域（８０００００ｈ～８０３ＦＦＦｈ）にアクセスする場合のみ、ロジック内蔵ＤＲＡＭに対してチップセレクト信号／ＣＳを活性化させる必要がある。

【０１１３】

図２４は、実施の形態５のロジック内蔵ＤＲＡＭの制御を説明するための動作波形図である。

【０１１４】

図２４を参照して、時刻ｔ１まではクロック信号ＣＬＫに同期した通常のＤＲＡＭに対するアクセスが行なわれる。

【０１１５】

時刻ｔ１において制御信号ＡＤＤ＿ＬがＨレベルになると、ロジック回路に対するコマンド制御モードに入る。以降、クロック信号ＣＬＫに同期してアドレス信号ＡＤＤによって指定されたレジスタにデータの授受が行なわれる。図２４の場合には、追加された制御信号／ＷＥ＿ＬがＬレベルであるので、コマンド制御

用レジスタにコマンド入力がなされる。

【０１１６】

［実施の形態５の変形例］

図２５は、実施の形態５の変形例を説明するための図である。

【０１１７】

通常のＤＲＡＭアドレス空間をアクセスするときには、マイクロコンピュータ１３２は、ＣＰＵコア１３４から指定されたアドレスに対して、メモリコントローラ１３６がマルチプレクス回路１４０を用いてＸアドレスおよびＹアドレスをアドレス信号Ａ０～Ａ１３が伝達されるアドレスバスにマルチプレクスして出力する。

【０１１８】

しかし、図２３で示したように、ＤＲＡＭ空間とは異なる領域にロジック制御領域が割当てられる場合には、メモリコントローラ１３６は、マルチプレクス回路１４０を用いないでそのままアドレスを外部バスインターフェイス回路１４２から出力することになる。

【０１１９】

この場合には、アドレス信号Ａ０～Ａ２０のうち、マルチプレクスされた後有効となっているピン数に対応するアドレス信号Ａ０～Ａ１３を用いてＳＲＡＭと同様な方法でアドレスの指定がなされる。この場合、信号Ａ１４～Ａ２０は何であってもかまわない状態、いわゆる「Don't Care」の状態である。このようなアドレス信号Ａ０～Ａ２０が／ＣＳの活性化とともに指定されると、応じてロジック内蔵ＤＲＡＭ１２１が処理を行なう。

【０１２０】

ただし、この場合も、マイクロコンピュータが、アドレスビットＡ２３＝“１”である他のアドレス領域を使用する可能性がある場合には、ロジック制御領域（８０００００ｈ～８０３ＦＦＦｈ）にアクセスする場合のみ、ロジック内蔵ＤＲＡＭに対してチップセレクト信号／ＣＳを活性化させる必要がある。

【０１２１】

かかる場合には、ロジック内蔵ＤＲＡＭ１２１は、レジスタ１２６の一部にア

ドレスの変化を検知するＡＴＤ（Address Transition Detect）回路１３０を設ける。

【０１２２】

図２６は、実施の形態５の変形例の動作を説明するための動作波形図である。

この場合には、時刻ｔ１までは、制御信号ＡＤＤ＿ＬはＬレベルであり、通常のＤＲＡＭアクセスがなされるが、ＡＤＤ＿ＬがＨレベルになると、ロジック回路に対するコマンド制御モードに入る。このとき、／ＷＥ＿ＬがＨレベルの場合には、ライトモードが指定されて／ＷＥ＿ＬがＨレベルの場合にはリードモードが指定される。

【０１２３】

そして、アドレス信号Ａ０～Ａ１３によって指定されるアドレスＡＤＤが変化すると、ＡＴＤ回路１３０がこれを検知し、クロック信号ＣＬＫにかかわらず内部の動作クロックを発生しＤＱに与えられる信号を内部のコマンドレジスタにライトしたり、アドレスで指定されるレジスタの内容をＤＱ端子からリードすることができる。

【０１２４】

以上説明したように、半導体記憶装置１２１の制御信号／ＷＥ＿Ｌを受ける端子とマイクロコンピュータ１３２側のＳＲＡＭ制御用に出力される信号Ａ２３が出力される端子とを接続することで、半導体記憶装置１２１をＳＲＡＭのように制御すれば特殊な機能をマイクロコンピュータ側に入れる必要がない。マイクロコンピュータは、外部拡張したＳＲＡＭ等のメモリに対してデータの書込または読出を行なう通常のコマンドを実行すれば、半導体記憶装置１２１に搭載したロジック回路を制御することができる。

【０１２５】

［実施の形態６］

実施の形態６では、より具体的な暗号ロジック内蔵ＤＲＡＭについて説明する。以降、この暗号ロジック内蔵ＤＲＡＭをセキュリティーＳＤＲＡＭ（ＳｃＲＡＭ）と称する。

【０１２６】

図２７は、ＳｃＲＡＭ２００の構成を示したブロック図である。

図２７を参照して、ＳｃＲＡＭ２００は、外部からクロック信号ＣＬＫを受けるクロックバッファ２０２と、外部とデータ信号ＤＱを授受するための入出力バッファ２０４と、外部からアドレス信号ＡＤＤ，コマンド信号ＣＭＤおよび信号ＣＲＹＰを受ける入力バッファ２０６とを含む。

【０１２７】

ＳｃＲＡＭ２００は、さらに、入力バッファ２０６の出力に応じて動作モード情報を保持するモードレジスタ２０８と、入力バッファ２０６およびモードレジスタ２０８の出力に応じてＳｃＲＡＭの制御を行なうＤＲＡＭ制御アドレスカウンタ２１０と、ＤＲＡＭ制御アドレスカウンタ２１０の制御の下にデータ保持動作を行なうＤＲＡＭ部２１２とを含む。

【０１２８】

入出力バッファ２０４とＤＲＡＭ部２１２とは内部バスｍｂｕｓ［１５：０］で接続される。ＤＲＡＭ部２１２は、複数のバンクを備えており、各バンクはメモリアレイ、ロウデコーダ、コラムデコーダおよびセンスアンプ、入出力制御回路を含んでいる。

【０１２９】

ＳｃＲＡＭ２００は、さらに、セレクタ２１４と、レジスタＲＥＧ０，ＲＥＧ１，ＲＥＧ２と、カウンタ２２０，２２４と、制御回路２２２と、暗号ロジック２２８とを含む。

【０１３０】

モードレジスタ２０８には、ＳＤＲＡＭの制御コマンドであるモードレジスタセット（ＭＲＳ）時のパラメータが保存される。このパラメータとしては、ＳＤＲＡＭのモード設定だけでなく、制御レジスタＲＥＧ０～ＲＥＧ２のアクセスのイネーブル／ディスエーブルも設定できる。また、ＭＲＳが入力されると制御レジスタＲＥＧ０～ＲＥＧ２および暗号ロジック２２８がリセットされる。

【０１３１】

ＳｃＲＡＭ２００には、暗号ロジック機能を制御するために３種類の制御レジスタＲＥＧ０～ＲＥＧ３が設けられている。

【０１３２】

制御レジスタＲＥＧ０は暗号ロジックを制御するコマンドや、モードを制御するためのレジスタである。制御レジスタＲＥＧ１は、暗号ロジックの入力データの保持をするレジスタである。制御レジスタＲＥＧ１の保持容量は最大４ｋｂである。

【０１３３】

制御レジスタＲＥＧ２は、暗号ロジックの出力結果を保持するレジスタである。制御レジスタＲＥＧ２もその保持容量は最大４ｋｂである。

【０１３４】

次に、制御レジスタＲＥＧ０～ＲＥＧ２に対するアクセス方法を説明する。

外部から制御レジスタをアクセスすることにより、ＳｃＲＡＭ２００の内蔵する暗号ロジックの制御、データの入出力、低消費電力化モードの制御を行なうことができる。

【０１３５】

図２８は、制御レジスタの設定に応じたメモリマップの状態変化を説明するための図である。

【０１３６】

図２８を参照して、ＳｃＲＡＭの内蔵する暗号機能を制御するには、２通りの方法がある。

【０１３７】

まず第１の方法は、制御レジスタアクセスイネーブル信号ＣＲＹＰとして外部から１を入力することである。これにより、Ｘ＝＃３ＦＦＦのページが制御レジスタ領域となる。

【０１３８】

第２の方法は、制御レジスタアクセスイネーブル信号ＣＲＹＰが０の場合に、ＳＤＲＡＭのモード設定のためＭＲＳコマンドを入力するときに、アドレスビットＡ１０として１を入力することである。この場合は、アドレスビットＡ１１が０の場合には、Ｘ＝＃３ＦＦＦのページが制御レジスタ領域になる。また、アドレスビットＡ１１が１の場合には、Ｘ＝＃００００のページが制御レジスタ領域

となる。

【０１３９】

ＳｃＲＡＭの制御レジスタを使用しない場合は、ＳＤＲＡＭのモードを設定するための通常のＭＲＳコマンドをＡ１０＝.0に設定することにより入力する。この場合、制御レジスタアクセスイネーブル信号ＣＲＹＰ＝０にする必要がある。信号ＣＲＹＰやＭＲＳコマンド入力からｔＲＳＣ以降には、ＳｃＲＡＭは新たなコマンドに対して動作可能となる。

【０１４０】

制御レジスタアクセスがイネーブルの期間、特定のロウアドレス（Ｘ＝＃３ＦＦまたは、Ｘ＝＃０）のアドレス空間に、定められたデータをライト／リードすることによって、制御用レジスタＲＥＧ０～ＲＥＧ２にアクセスすることができる。この間は、暗号をロジック制御用に割当てられた４ｋビットのアドレス空間をメモリとして用いることはできない。それ以外の空間については、通常のメモリ領域として外部からアクセスすることが可能である。

【０１４１】

ここで、制御レジスタアクセスに対応するアドレス空間に外部からアクセスした場合には、ＤＲＡＭ部２１２に対してはアクセスが行なわれない。したがって、制御レジスタアクセスのイネーブル状態から抜ければ、制御レジスタ領域であった特定のロウアドレスに対応するメモリ空間を通常のメモリ空間としてアクセスすることができる。制御レジスタアクセスのイネーブル状態から抜ける前にレジスタに設定した値は、信号ＣＲＹＰを０にして動作モードから抜けた場合には保持される。しかし、ＭＲＳコマンドを用いてモードから抜けた場合には、レジスタに設定した値はリセットされる。すなわち、ＭＲＳコマンドを入れることにより、レジスタをリセットすることができる。

【０１４２】

制御用レジスタＲＥＧ０～ＲＥＧ２に対するアクセスは、制御用レジスタに割当てられたアドレス空間内で、汎用ＳＤＲＡＭと同じシーケンスでアクセスすることにより行なわれる。制御レジスタからの読出データは、ＳＤＲＡＭのモードレジスタセット時に設定された同じＣＡＳレイテンシで出力されるが、制御用の

レジスタへのアクセス時のバースト長は１に固定される。

【０１４３】

次に、図２７のモードレジスタ２０８について説明する。

図２９、図３０、図３１は、図２７に示したモードレジスタ２０８を説明するための図である。

【０１４４】

図２９を参照して、モードレジスタセット命令はクロック信号ＣＬＫの立上がり時にコマンド信号ＣＭＤに含まれる信号／ＣＳ，／ＲＡＳ，／ＣＡＳ，／ＷＥをすべてＬレベルに設定することにより与えられ、このときにアドレス信号ＡＤＤに含まれるアドレスビットＢＡ０，ＢＡ１，Ａ０～Ａ１１で設定される値が図３０に示す各ビットに書込まれる。ただし、アドレスビットＡ８，Ａ７は、０に設定される。他のビットは図３１で示すように種々の設定に割当てられている。

【０１４５】

モードレジスタセットではＳＤＲＡＭのモード設定、ＳＤＲＡＭのローパワーモード設定、および制御レジスタのアクセスを行なうことができる。

【０１４６】

ＳＤＲＡＭのモード設定では、バースト長、バーストタイプ、および／ＣＡＳレイテンシをプログラムすることができる。

【０１４７】

ＳＤＲＡＭのローパワーモード設定では、非パワーダウンモード時のプリチャージスタンバイ電流を低減することができる。ただし、このモードを使用するには、入力信号のセットアップタイムを５ｎｓ以上にする必要がある。

【０１４８】

制御レジスタのアクセスでは、モードレジスタセット時に、ビットＡ１０を１にすると、暗号機能を制御するためのレジスタ空間が現われる。この方法は、信号ＣＲＹＰを入力する端子の制御ができないために、この端子を０に固定したシステムに適している。制御レジスタへのアクセスは、ＳＤＲＡＭのアクセスシーケンスと同じで、同じ／ＣＡＳレイテンシでデータが出力される。しかし、制御レジスタのアクセスは常にバースト長が１に固定されている。

【０１４９】

モードレジスタセットによりセットされたデータは、次のＭＲＳコマンドが入力されるまでモードレジスタに格納される。次のＭＲＳコマンドは、両バンクが非活性化状態にあれば入力できる。ＭＲＳコマンドからｔＲＳＣ後には、ＳＤＲＡＭは新たなコマンドに対して動作可能となる。また、ＭＲＳコマンドが入力されると制御レジスタがリセットされる。制御レジスタの内容を保持したまま、制御レジスタアクセスのディスエーブルとイネーブルとを切換えるには、ＳＤＲＡＭのモードレジスタセット時にビットＡ１０を０にして信号ＣＲＹＰの制御を行なうことで実現することができる。

【０１５０】

図３２は、ＳｃＲＡＭの暗号制御エントリ・エグジットに関連する状態遷移図である。

【０１５１】

電源投入がされると初期状態３４０にＳｃＲＡＭの状態が遷移する。続いて信号ＣＲＹＰを１にすると、暗号制御がイネーブルな状態３４４に遷移する。一方信号ＣＲＹＰが０の場合であっても、モードレジスタセットコマンドによりビットＡ１０を１に設定することにより暗号制御イネーブル状態３４４に遷移させることができる。

【０１５２】

パワーオンの初期状態３４０において信号ＣＲＹＰを０に設定し、モードレジスタコマンドによってビットＡ１０を０にすると暗号制御ディスエーブルな状態３４２に遷移する。

【０１５３】

状態３４２から３４４に遷移させるためには、信号ＣＲＹＰを１にすることによる場合と、信号ＣＲＹＰが０の状態であってモードレジスタセットコマンドによりビットＡ１０を１に設定することによる場合とがある。

【０１５４】

一方、暗号制御イネーブル状態３４４から暗号制御ディスエーブル状態３４２に遷移させるには、暗号制御イネーブル状態３４４に信号ＣＲＹＰを１に設定し

て入った場合には逆に信号ＣＲＹＰを０に設定することにより遷移させることができる。また、信号ＣＲＹＰを０に設定し、モードレジスタセットコマンドでビットＡ１０を１に設定してイネーブル状態３４４に入った場合には、モードレジスタセットコマンドによりビットＡ１０を０に設定することによりディスエーブル状態３４２へと遷移させることができる。

【０１５５】

図３３は、制御レジスタアクセスの一例を示した動作波形図である。

図３３を参照して、制御レジスタアクセス領域としてＸ＝＃３ＦＦＦのページが割当てられた場合を示す。ＳＤＲＡＭのモードがＣＡＳレイテンシＣＬ＝３に設定されているので、レジスタ出力もＣＬ＝３のタイミングになっている。

【０１５６】

ここで、モードレジスタセットにより設定されたバースト長ＢＬによらず、レジスタアクセスに関しては、バースト長は１に固定される。したがって、リード／ライトコマンドとコラムアドレスとを毎サイクル入力する必要がある。

【０１５７】

図３４～図３７は、制御レジスタのアドレスマップを示した図である。

図３４はコラムアドレスがｈ００，ｈ０１の場合を示し、図３５は、コラムアドレスがｈ０２の場合を示し、図３６は、コラムアドレスがｈ０３，ｈ０４，ｈ０５，ｈ０６の場合を示す。図３７は、コラムアドレスがｈ１３～ｈ２０の場合について示す。

【０１５８】

これらのＸアドレスはＸ＝ｈ３ＦＦＦまたはＸ＝ｈ０いずれかに初期設定された値である。

【０１５９】

次にＳｃＲＡＭの内蔵する暗号機能の特徴について説明する。

ＳｃＲＡＭは、ネットワーク上のセキュリティ確保のために使われている、主要な暗号方式のアクセラレータを内蔵している。また、ＳｃＲＡＭは、電子認証で用いられる公開鍵方式と認証後のデータ送受信で用いられる秘密鍵暗号方式の機能をサポートしている。これらは、図２７に示す専用の暗号ロジック２２８で

処理するので、低消費電力で高速暗号処理が必要なシステムに適する。

【０１６０】

サポートする暗号方式については、図９で示した場合と同様であり、公開鍵暗号方式としてＲＳＡを、秘密鍵暗号方式としてＤＥＳとトリプルＤＥＳとをサポートしている。さらに、秘密鍵暗号方式では、主要ブロック暗号モードであるＥＣＢ，ＣＢＣ，ＯＦＢ，ＣＦＢ－６４をサポートしている。

【０１６１】

一般的なネットワークだけでなく、インターネットでも、これらの暗号方式は主要な暗号方式として用いられている。主要なブラウザであるネットスケープコミュニケータやインターネットエクスプローラなど、暗号化電子メール方式であるＳ／ＭＩＭＥにも対応することができる。今後の拡大が期待される電子商取引市場では、これらの暗号方式を用いたセキュリティの確立が重要になると考えられる。また、携帯電話への運用が予想されるワイヤレスアプリケーションプロトコル（ＷＡＰ）でも上述の暗号化方式がサポートされるため、ＳｃＲＡＭは、さまざまなシステムに幅広い適合性がある。

【０１６２】

ＳｃＲＡＭは、アプリケーションの適合性を高めるため、内部暗号ロジックにより、暗号化でクリティカルな処理のみを受け持つ。すなわち、ハッシュ、データエンコーディング、パディングなどの処理は、従来どおりソフトウェア側で受け持つことになり、アプリケーション側の自由度を高めるように考慮されている。また、ＲＳＡでは、ソフトウェア処理で要する処理時間の大部分を占めていた次のａ），ｂ）の演算のみを処理する。

【０１６３】

ａ）　ＲＳＡによる電子認証を高速化するため、

べき乗剰余演算　M^e　ｍｏｄ　Ｎ、

モンゴメリー乗算剰余演算　$X*Y*R^{-1}$　ｍｏｄ　Ｎ、

剰余演算　Ｙ　ｍｏｄ　Ｎ

を実施する。

【０１６４】

ｂ）　暗号化通信の高速化をするために、トリプルＤＥＳ、ＤＥＳ（ＣＢＣ，ＥＣＢ，ＯＦＢ，ＣＦＢ－６４）の演算を行なう。ただし、最終テキストブロック部のパディング処理は、規格によってさまざまであるので、適宜、ソフトウェアで処理する必要がある。

【０１６５】

続いて、暗号処理速度について述べる。

アドレス処理専用ロジックとＤＲＡＭのワンチップ化によって、高速化と低消費電力化とを実現している。その結果、携帯端末に適した低電源電圧（２．５Ｖ系）で、

１０２４ｂｉｔ　ＲＳＡ暗号署名処理時間：１００－２００ｍｓ

約６０Ｍｂｐｓのトリプルｄｅｓ処理。ＤＥＳであれば、約１８０Ｍｂｐｓ。の性能を実現することができる。

【０１６６】

また、ＳｃＲＡＭは、特定のアドレス空間をアクセスすることで、暗号ロジック部分を制御しているので、汎用ＳＤＲＡＭとピン交換を実現することができる。また、暗号機能をディスエーブルにすれば、ＳＤＲＡＭとしての機能のみを使用することもできる。

【０１６７】

続いて暗号機能制御方法について説明する。

先に説明したように、ＳｃＲＡＭに内蔵している暗号機能の制御は、制御レジスタに対してアクセスを行なうことで実行することができる。制御レジスタにアクセスするには、モードレジスタセット時に所定のアドレスを入力するか、信号ＣＲＹＰが与えられる端子を１に設定して、特定のアドレスにアクセスすることによって制御レジスタにアクセスすることができる。ここで、制御レジスタに割当てられたデフォルトのアドレス空間は、Ｘ＝ｈ３ＦＦＦのページである。また、ＭＲＳコマンド入力時に、ビットＡ１０，Ａ１１をともに１に設定すれば、Ｘ＝ｈ０のページに制御レジスタを割当てることもできる。

【０１６８】

しかし、ファームウエア設計では、制御レジスタアクセスのために予約された

空間を、それ以外の用途で使用しないことが要求される。たとえば、アプリケーションやカーネルにこの空間を割当てることを禁止しなければならない。カーネルに関しては、ブート時に割当てられないように注意する必要がある。

【０１６９】

続いて、システム設計の例を説明する。

図３８は、信号ＣＲＹＰを与える端子を制御可能なシステムを説明するための図である。

【０１７０】

図３８を参照して、一般のマイコン（ＭＣＵ）が備えているＩ／Ｏポートを、ＣＲＹＰ信号を受ける端子に接続することができるシステムについて例示している。この構成では、システムのブート前にＣＲＹＰ端子を０にすることができれば、制御レジスタに割当てられたアドレス空間が現われていないので、プログラムを初期ロードする空間には制約がない。プログラムがロードされた領域がＸ＝ｈ３ＦＦＦを含んでいる場合には、その後ＣＲＹＰ端子を１に設定して、制御レジスタに割当てられたアドレス空間をＸ＝ｈ０のページに変更する必要がある。

【０１７１】

図３９、図４０は、ＣＲＹＰ端子を制御不可能なシステムについて説明するための図である。

【０１７２】

図３９を参照して、ＣＲＹＰ端子に与える値を０に固定した場合には、ＳｃＲＡＭのモードレジスタセット（ＭＲＳ）入力時に、ビットＡ１０を１にして制御レジスタへのアクセスをイネーブルにする。このときに、ビットＡ１１でプログラムがロードされていない空間を選択する。

【０１７３】

図４０を参照して、ＣＲＹＰ端子に与える値を１に固定した場合には、Ｘ＝ｈ３ＦＦＦのページに制御レジスタへのアクセス空間が割当てられるので、この空間を避けてプログラムのロードを行なう必要がある。

【０１７４】

図４１は、制御レジスタへの設定の説明をするための動作波形図である。

図４１を参照して、制御レジスタの設定に関して信号入力の一例が示される。制御レジスタへのアクセスでＤＲＡＭと唯一異なる点は、ＭＲＳの設定によらずバースト長が１になることである。それ以外に関しては、ＤＲＡＭと同じタイミング、かつ、同じシーケンスで、制御レジスタに対してアクセスを行なう。

【０１７５】

図４１では、制御レジスタにアクセスするためのアドレス空間がＸ＝ｈ３ＦＦＦの場合を例として示している。

【０１７６】

まず時刻ｔ１において、制御レジスタにアクセスするためのアドレスＸ＝ｈ３ＦＦＦが入力される。

【０１７７】

続いて時刻ｔ２において、ソフトリセットがされる。

時刻ｔ３では、モード設定（１）がなされる。モード設定（１）は、秘密鍵暗号方式としてＤＥＳ－５６を選択し、ＣＢＣモードで処理を行なうモード設定である。

【０１７８】

続いて時刻ｔ４ではモード設定（２）が行なわれる。モード設定（２）は、暗号化、ＲＥＧ１とＲＥＧ２のアドレスカウンタをリセット。初期値としてＩＶを使う。というモードが設定される。

【０１７９】

時刻ｔ５～ｔ６では、秘密鍵が入力される。

時刻ｔ６～ｔ７では、イニシャルベクトルＩＶが入力される。

【０１８０】

時刻ｔ７～ｔ８では、８バイト単位の平文を入力し、平文入力後時刻ｔ８においてＥＯＦ（エンドオブファイル）の入力が行なわれる。

【０１８１】

そして時刻ｔ９では、フラグ領域に対するリードを行ない、暗号ロジックが処理中か否かをチェックする。

【０１８２】

このチェック結果はＣＡＳレイテンシでデータ信号ＤＱとして読出される。

続いて、ＳｃＲＡＭがサポートする秘密鍵暗号方式について説明する。

【０１８３】

図４２～図４４は、暗号化処理の基本単位について示した概略図である。

図４２は、鍵の長さが５６ｂｉｔのＤＥＳを示し、図４３は、鍵の長さが１１２ｂｉｔのトリプルＤＥＳ方式を示し、図４４は、鍵の長さが１６８ｂｉｔのトリプルＤＥＳ方式について示している。ＳｃＲＡＭでは、秘密鍵暗号化方式としてＤＥＳとトリプルＤＥＳとをサポートしている。インターネットのセキュリティソケットレイヤ、Ｓ／ＭＩＭＥの電子メール、ワイヤレスアプリケーションプロトコルでこれらの暗号化方式は利用されている。なお、トリプルＤＥＳは、ＤＥＳを暗号化－復号化－暗号化の３回処理を行なったものである。

【０１８４】

図４５～図４７は、復号化処理の単位について示した概略図である。

図４５は、図４２の暗号化に対応する復号化を示し、図４６は、図４３の暗号化に対応する復号化を示し、図４７は、図４４の暗号化に対応する復号化を示す。

【０１８５】

続いて、ＳｃＲＡＭがサポートする秘密鍵暗号の暗号利用モードについて説明する。例として、ＥＣＢ，ＣＢＣの２つのモードについて説明する。

【０１８６】

図４８、図４９は、ＥＣＢモードについて説明するための図である。

図４８、図４９を参照して、ＥＣＢモードは基本モードであり、暗号／復号処理基本単位に当たる。暗号化では、通常のデータ（平文）Ｍを図４８に示すように６４ビットごとに分解したブロックＭｉ（Ｍ＝Ｍ１、Ｍ２、Ｍ３…）を送信者と受信者のみが共通に持つ秘密の鍵と呼ばれるデータＫを用いて、各ブロックごとに暗号化処理を行なう。そして、６４ビットの暗号文Ｃｉ（Ｃ＝Ｃ１、Ｃ２、Ｃ３…）が生成される。復号化では、図４９に示すように、６５ビットの暗号文Ｃｉを受取り、暗号化に用いたものと同じ鍵データＫを用いて、平文Ｍｉ（Ｍ＝Ｍ１、Ｍ２、Ｍ３…）を生成する。

【０１８７】

次にＣＢＣモードについて説明する。

図５０は、ＣＢＣモードの演算を説明するための図である。

【０１８８】

図５０を参照して、ＣＢＣモードでは、まず暗号化は、平文Ｍを６４ビットごとに分解したブロックＭｉをＥＣＢモードと同様に暗号化を行なう。そして、さらに、この暗号文ブロックＣｉと、次のブロックＭｉ＋１との排他的論理和を次の暗号化の入力とする。これを繰返して次々と連鎖させるのである。

【０１８９】

一方、復号化は、暗号ブロック文ＣｉをＥＣＢモードと同様に復号化した結果をＭｉとし、Ｃｉを次の暗号文ブロックＣｉ＋１の復号結果との排他的論理和をとり、出力平文ブロックＭｉ＋１とする。これを繰返して次々と連鎖させるのである。なお、図５０において、平文はＭｉ、暗号文はＣｉ（ｉ＝１，２，…）、暗号鍵Ｋを用いた暗号化をＥｋ、復号化をＤｋとする。

【０１９０】

また、ＩＶ（イニシャルベクトル）は初期値であり、最初の暗号化と復号化の際に用いられる。ＩＶは、暗号側と復号側とで同一の値を用いる。ＩＶの値は、第三者に知られてもよいので、ＩＶは送信者と受信者との間で秘密に送る必要がない。ＩＶの値を変えると、同じメッセージから異なった暗号文が生成される。

【０１９１】

図５１は、ＣＢＣモードにおける暗号化の概要を示した概念図である。

図５２は、ＣＢＣモードにおける復号化の概要を示した概念図である。

【０１９２】

図５１、図５２を参照して、ＳｃＲＡＭに一度に入力可能な平文長はレジスタＲＥＧ１のサイズである４ｋビットである。したがって、４ｋビットよりも長い平文を処理する場合には、直前の暗号文ブロックＣｉが初期値になるように制御レジスタに対して設定を行なう。

【０１９３】

本明細書の実施の形態では、ＳＤＲＡＭに本発明を適用した場合を例として示

したが、ＳＤＲＡＭに制限されるものではなく、非同期型のＤＲＡＭ、たとえばＥＤＯ（Extended Data Out）ＤＲＡＭ等にも本発明を適用することも可能である。また、同期型の他のＤＲＡＭ、たとえばＤＤＲ（Double Data Rate）型のインタフェースを有するＤＲＡＭ等であっても本発明を適用することが可能である。

【０１９４】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【０１９５】

【発明の効果】

請求項１～３に記載の半導体記憶装置は、汎用的なメモリに対してデータ、アドレスおよび制御信号を与えるのと同様なシーケンスで信号を与えることで内蔵するロジック回路を制御することができ、既存のシステムに大きな変更を加える必要がなく、容易に制御することができる。

【０１９６】

請求項４に記載の半導体記憶装置は、請求項３に記載の半導体記憶装置の奏する効果に加えて、通常のメモリに対する読出を所定アドレスを指定して行なうことで、内蔵するロジック回路の動作状態を確認することができる。

【０１９７】

請求項５に記載の半導体記憶装置は、請求項３に記載の半導体記憶装置の奏する効果に加えて、内蔵するロジック回路が暗号処理を行なう場合に容易に制御を行なうことができる。

【０１９８】

請求項６に記載の半導体記憶装置は、請求項２に記載の半導体記憶装置の奏する効果に加えて、短時間で複数のモード設定を行なうことができる。

【０１９９】

請求項７に記載の半導体記憶装置は、請求項２に記載の半導体記憶装置の奏す

る効果に加えて、予約領域が様々なマイコンシステムに対応できる。

【０２００】

請求項８に記載の半導体記憶装置は、請求項１に記載の半導体記憶装置の奏する効果に加えて、既存のメモリと置き換えて使用することが可能である。

【０２０１】

請求項９に記載の半導体記憶装置は、請求項１に記載の半導体記憶装置の奏する効果に加えて、内蔵メモリを有効に活用することができる。

【０２０２】

請求項１０に記載の半導体記憶装置は、請求項９に記載の半導体記憶装置の奏する効果に加えて、特別な制御端子や命令がなくても内蔵メモリの保持データを内蔵ロジック回路に処理させることができる。

【０２０３】

請求項１１～１３に記載の半導体記憶装置の制御方法は、マイコンシステムにおいて、ロジック内蔵の半導体記憶装置を容易に制御することができる。

【０２０４】

請求項１４～１６に記載の半導体記憶装置は、最小限の制御端子の追加で、内蔵メモリにアドレスやデータを与える経路を有効に使用して、内蔵するロジック回路の制御を行なうことができる。

【図面の簡単な説明】

【図１】　本発明の実施の形態１の半導体記憶装置１の構成を示したブロック図である。

【図２】　実施の形態１のロジック内蔵半導体記憶装置のメモリマップの例を示した図である。

【図３】　外部から入力される信号がロジック回路へ伝達される様子を説明するための図である。

【図４】　実施の形態１の半導体記憶装置の標準的なタイミングを説明するための波形図である。

【図５】　実施の形態１の変形例であるロジック内蔵ＤＲＡＭ１０の構成を示すブロック図である。

【図６】　図５に示したロジック内蔵ＤＲＡＭ１０のメモリマップを示した図である。

【図７】　実施の形態２のロジック内蔵ＤＲＡＭ３０の構成を示すブロック図である。

【図８】　実施の形態２のロジック内蔵ＤＲＡＭに適用されるシステムのメモリマップを示した図である。

【図９】　図７の暗号演算ロジック７４がサポートする暗号方式を示した図である。

【図１０】　レジスタに割当てられるデータ例を示した第１の図である。

【図１１】　レジスタに割当てられるデータ例を示した第２の図である。

【図１２】　レジスタに割当てられるデータ例を示した第３の図である。

【図１３】　レジスタに割当てられるデータ例を示した第４の図である。

【図１４】　レジスタに割当てられるデータ例を示した第５の図である。

【図１５】　レジスタに割当てられるデータ例を示した第６の図である。

【図１６】　レジスタに割当てられるデータ例を示した第７の図である。

【図１７】　レジスタに割当てられるデータ例を示した第８の図である。

【図１８】　レジスタに割当てられるデータ例を示した第９の図である。

【図１９】　本発明のロジック内蔵ＤＲＡＭ９２とマイクロコンピュータ９０とが接続される様子を示した図である。

【図２０】　ロジック内蔵ＤＲＡＭの制御を説明するためのフローチャートである。

【図２１】　実施の形態４において割当てたメモリマップを示した図である。

【図２２】　実施の形態５のロジック内蔵ＤＲＡＭ１１１の構成を示した図である。

【図２３】　実施の形態５におけるマイクロコンピュータシステムのメモリマップを示した図である。

【図２４】　実施の形態５のロジック内蔵ＤＲＡＭの制御を説明するための動作波形図である。

【図２５】　実施の形態５の変形例を説明するための図である。

【図２６】　実施の形態５の変形例の動作を説明するための動作波形図である。

【図２７】　ＳｃＲＡＭ２００の構成を示したブロック図である。

【図２８】　制御レジスタの設定に応じたメモリマップの状態変化を説明するための図である。

【図２９】　図２７に示したモードレジスタ２０８を説明するための第１図である。

【図３０】　図２７に示したモードレジスタ２０８を説明するための第２図である。

【図３１】　図２７に示したモードレジスタ２０８を説明するための第３図である。

【図３２】　ＳｃＲＡＭの暗号制御エントリ・エグジットに関連する状態遷移図である。

【図３３】　制御レジスタアクセスの一例を示した動作波形図である。

【図３４】　制御レジスタのアドレスマップを示した第１図である。

【図３５】　制御レジスタのアドレスマップを示した第２図である。

【図３６】　制御レジスタのアドレスマップを示した第３図である。

【図３７】　制御レジスタのアドレスマップを示した第４図である。

【図３８】　信号ＣＲＹＰを与える端子を制御可能なシステムを説明するための図である。

【図３９】　ＣＲＹＰ端子を制御不可能なシステムについて説明するための第１の図である。

【図４０】　ＣＲＹＰ端子を制御不可能なシステムについて説明するための第２の図である。

【図４１】　制御レジスタへの設定の説明をするための動作波形図である。

【図４２】　暗号化処理の基本単位について示した第１の概略図である。

【図４３】　暗号化処理の基本単位について示した第２の概略図である。

【図４４】　暗号化処理の基本単位について示した第３の概略図である。

【図４５】　復号化処理の単位について示した第１の概略図である。

【図４６】　復号化処理の単位について示した第２の概略図である。

【図４７】　復号化処理の単位について示した第３の概略図である。

【図４８】　ＥＣＢモードについて説明するための第１図である。

【図４９】　ＥＣＢモードについて説明するための第２図である。

【図５０】　ＣＢＣモードの演算を説明するための図である。

【図５１】　ＣＢＣモードにおける暗号化の概要を示した概念図である。

【図５２】　ＣＢＣモードにおける復号化の概要を示した概念図である。

【図５３】　従来の、シンクロナスダイナミックランダムアクセスメモリ（ＳＤＲＡＭ）のピン配置を示した図である。

【図５４】　ＳＤＲＡＭの端子名と機能とを示した図である。

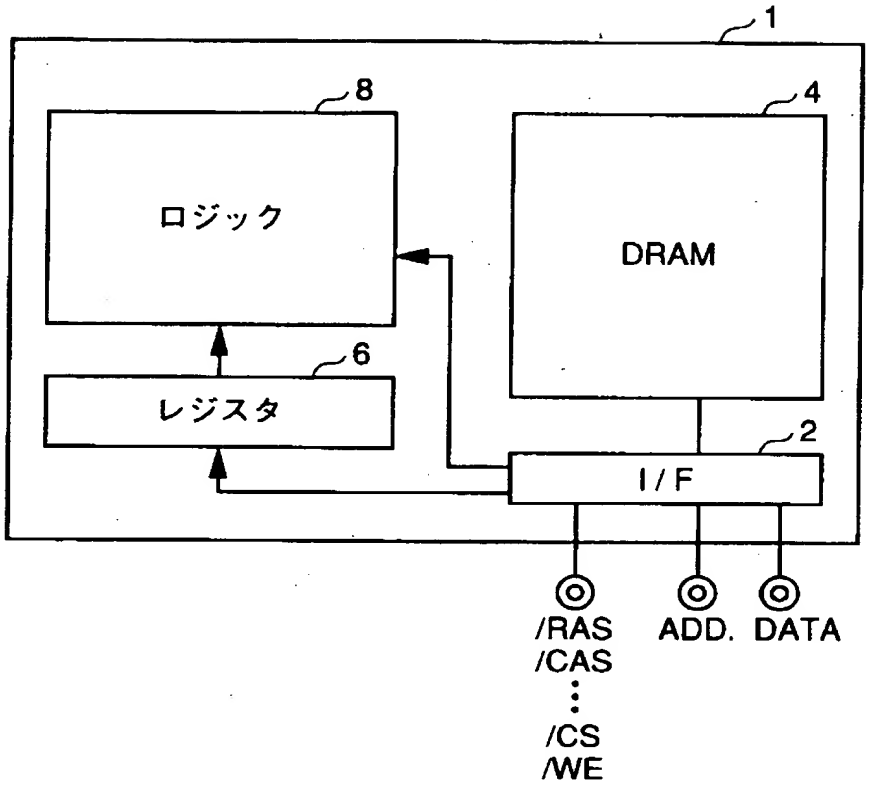
【図５５】　従来のロジック内蔵ＤＲＡＭの構成を示す図である。

【符号の説明】

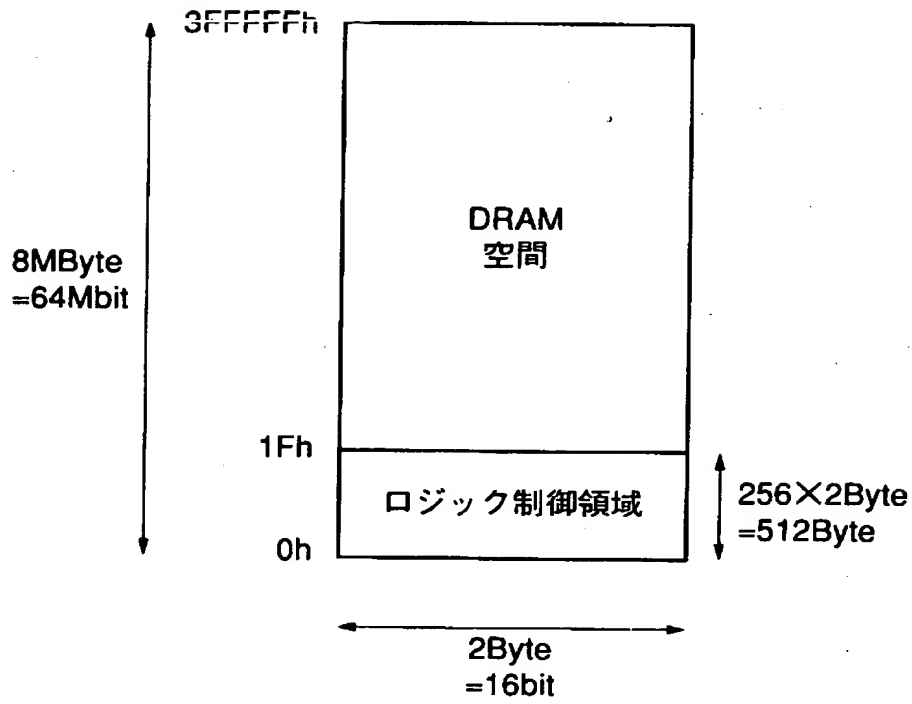
１　半導体記憶装置、２　インターフェイス部、３　バッファ、５　デコード回路、６，１４，１６，１１６，１２６　レジスタ、８，１１８　ロジック回路、１０，３０，９２，１１１，１２１　ロジック内蔵ＤＲＡＭ、１２　インターフェイス部、１８，２０　ロジック回路、３２　ＳＤＲＡＭ部、３４　ロジック部、３６　インターフェイス部、３８　ＤＲＡＭコア、４０　制御信号入力回路、４２　制御回路、４４　クロックバッファ、４６　アドレスバッファ、４８　マルチプレクサ、５０　モードレジスタ、５２　入出力回路、５４　メモリセルアレイ、５６　ロウデコーダ、６０　ライトドライバ、７２　レジスタ部、７４　暗号演算ロジック、７６　セレクタ、７８　制御レジスタ、８０　モードレジスタ、８２　ステータスレジスタ、８４，８６　データレジスタ、９０，１３２　マイクロコンピュータ、９４，１３４　ＣＰＵコア、９６　キャッシュメモリ、９８，１３６　メモリコントローラ、１００，１４２　外部バスインターフェイス回路、１０２　内部バス、１２１　半導体記憶装置、１３０　ＡＴＤ回路、１４０　マルチプレクス回路。

【書類名】　　図面

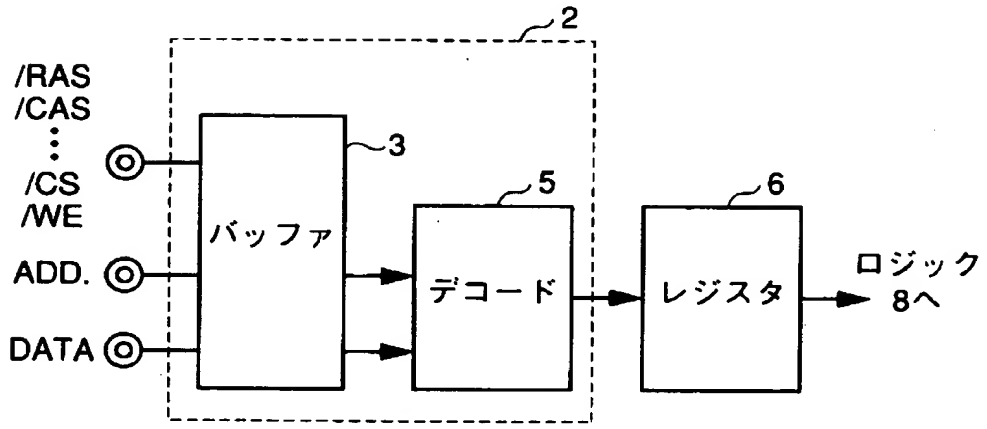
【図１】



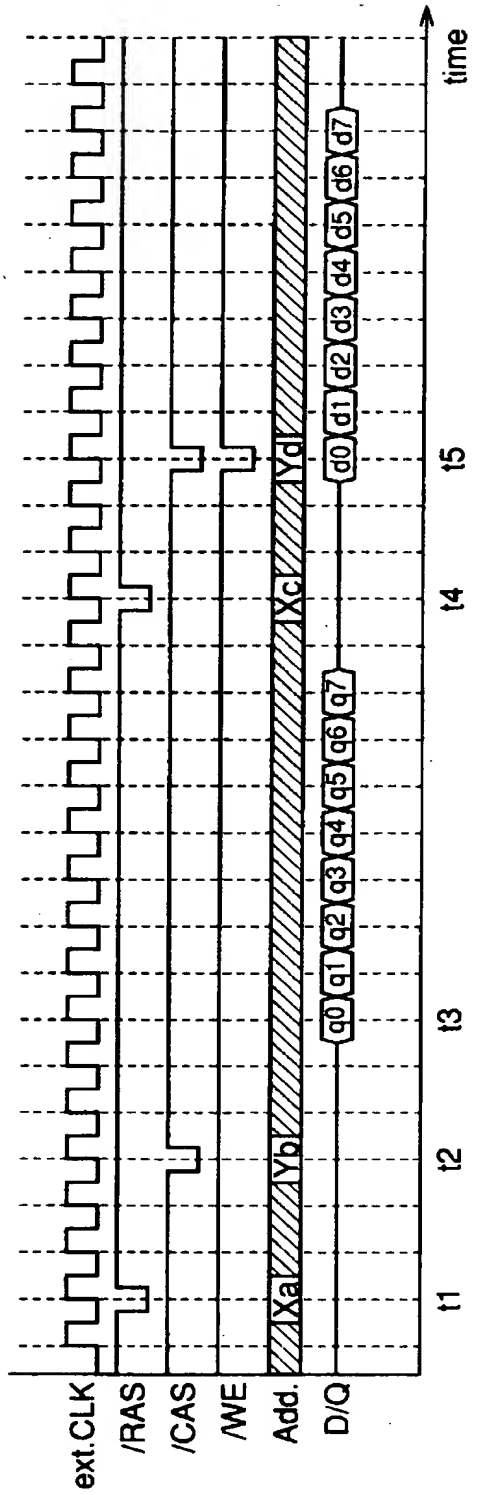
【図２】


3FFFFFh
8MByte
=64Mbit
DRAM
空間
1Fh
ロジック制御領域
0h
256×2Byte
=512Byte
2Byte
=16bit

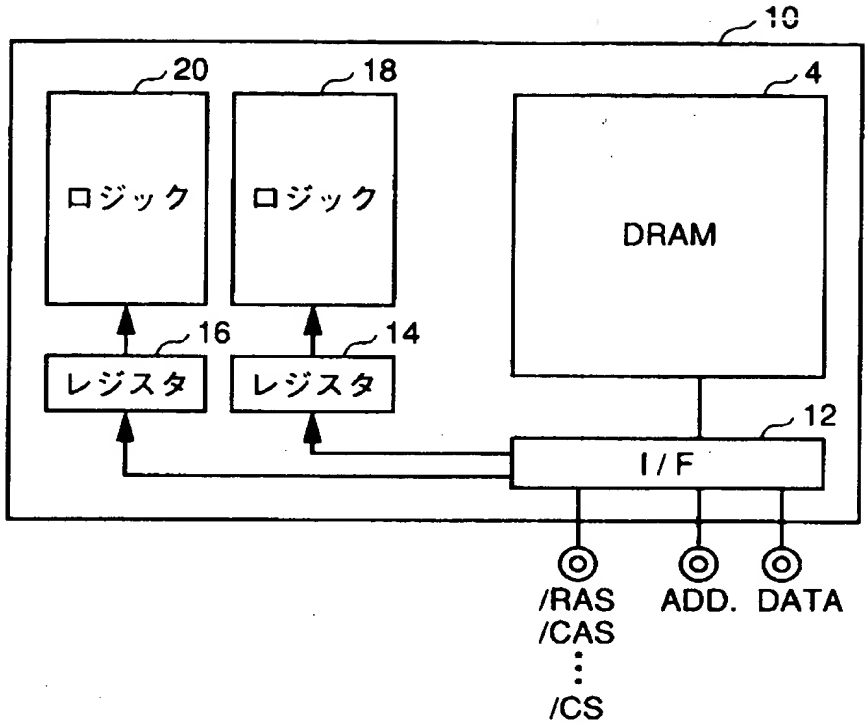
【図３】


2
/RAS
/CAS
/CS
/WE
ADD.
DATA
バッファ
3
デコード
5
レジスタ
6
ロジック
8へ

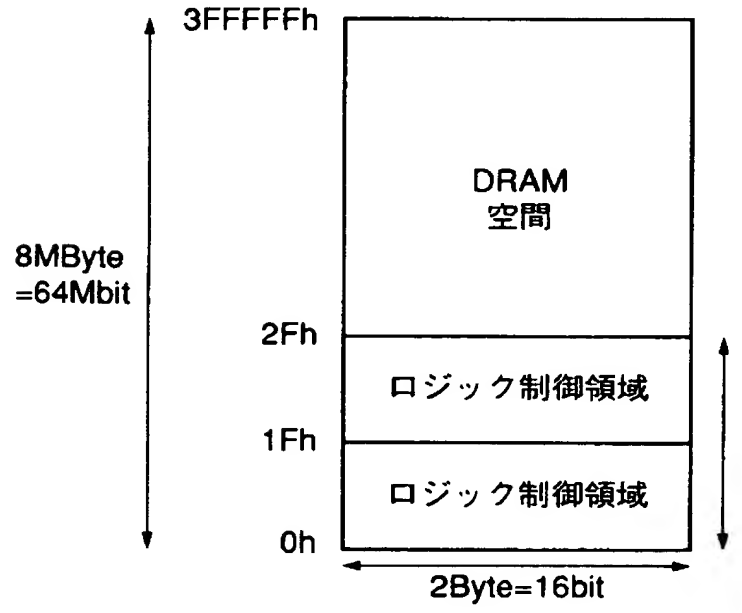
【図４】


time
t1
t2
t3
t4
t5
ext.CLK
/RAS
/CAS
/WE
Add.
D/Q
Xa
Yb
Xc
Yd
q0
q1
q2
q3
q4
q5
q6
q7
d0
d1
d2
d3
d4
d5
d6
d7

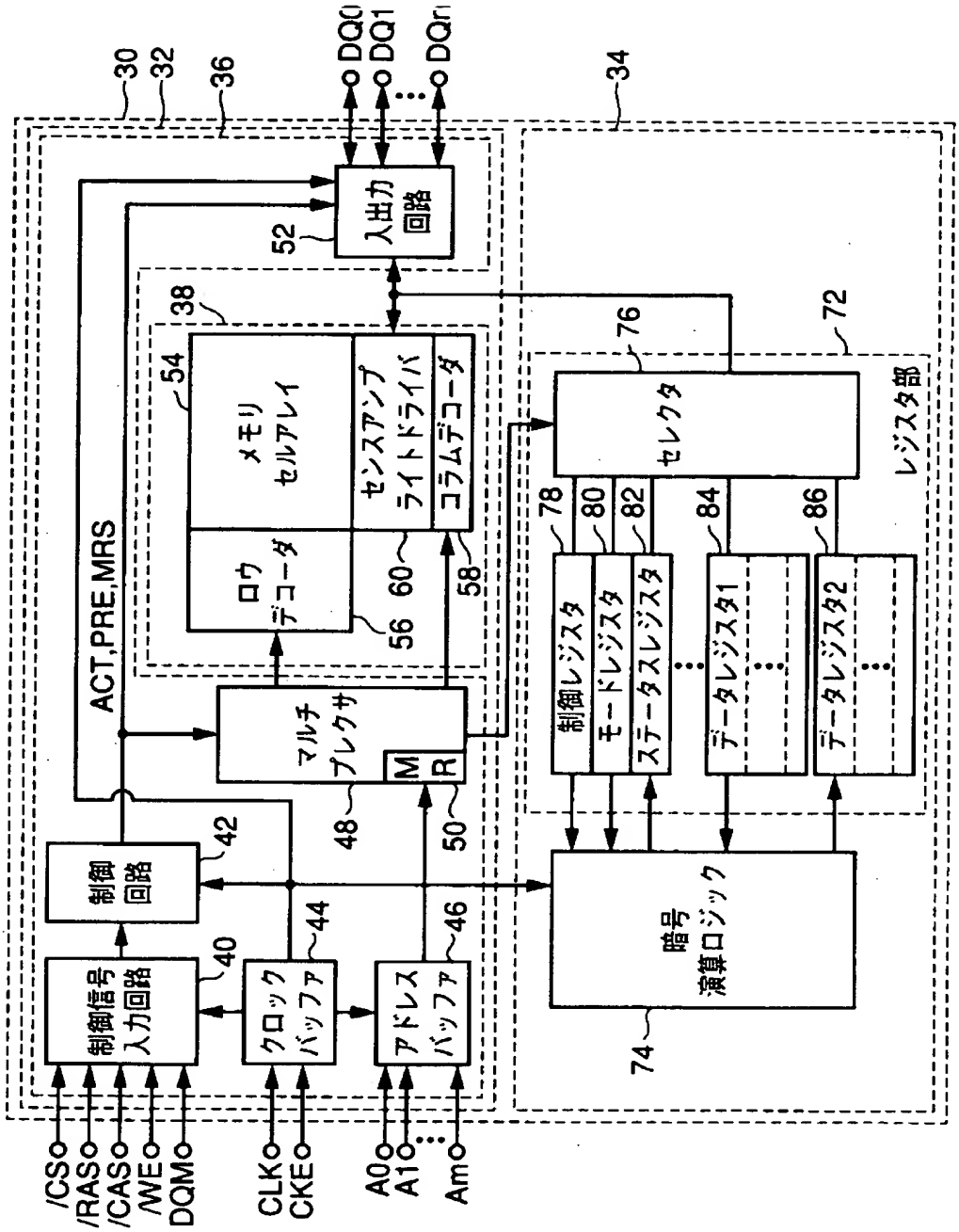
【図５】


10
20
18
4
ロジック
ロジック
DRAM
16
14
レジスタ
レジスタ
12
I/F
/RAS
/CAS
/CS
ADD.
DATA

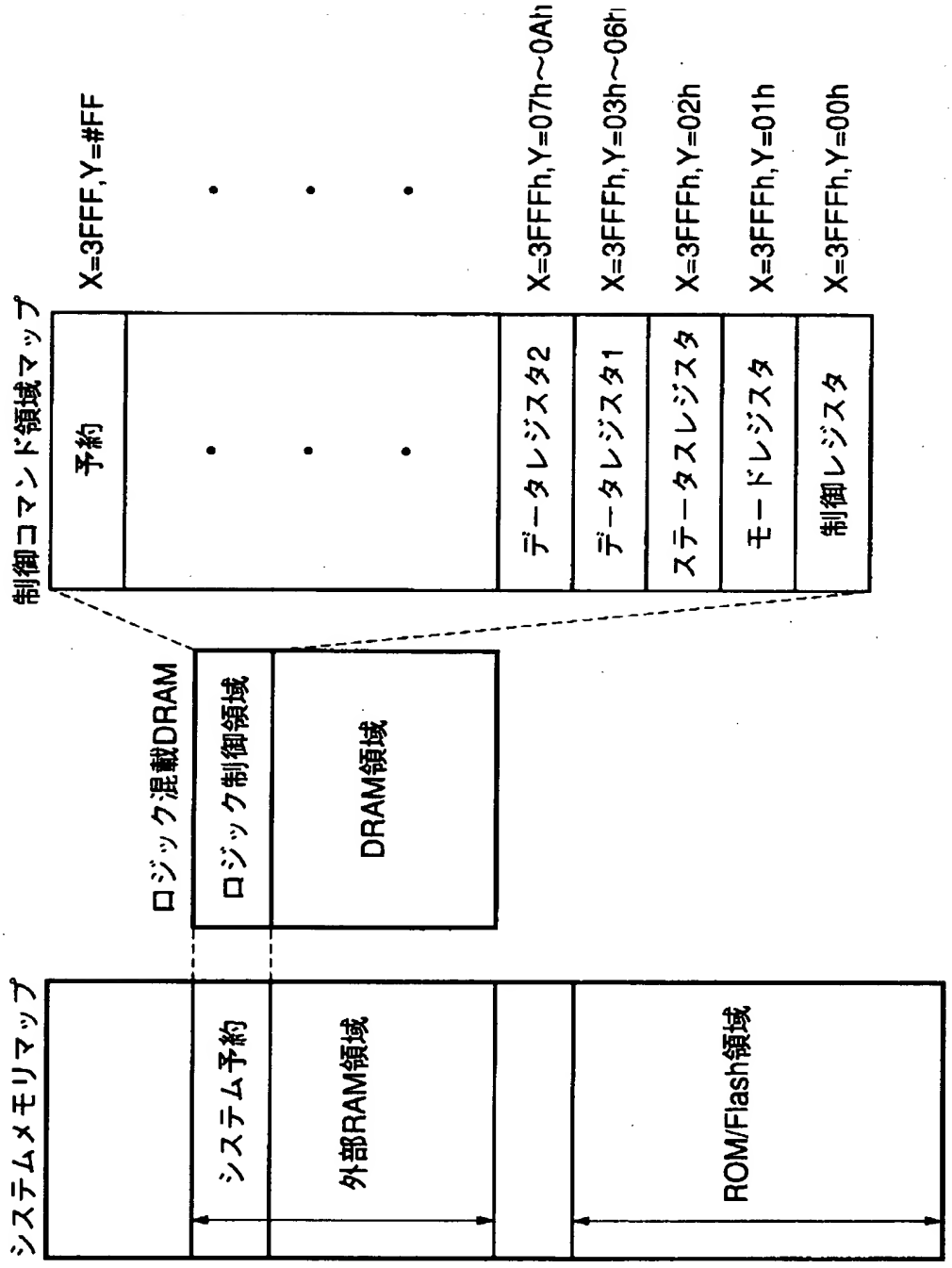
【図６】


3FFFFFh
DRAM
空間
8MByte
=64Mbit
2Fh
ロジック制御領域
1Fh
ロジック制御領域
0h
2Byte=16bit

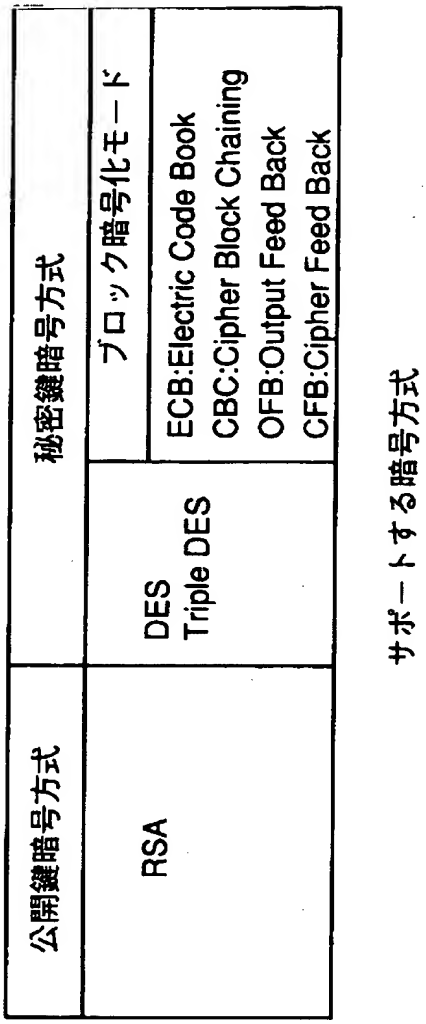
【図７】


30
32
36
34
DQ0
DQ1
DQn
入出力回路
52
38
54
メモリセルアレイ
センスアンプライトドライバ
コラムデコーダ
ロウデコーダ
56
60
58
ACT,PRE,MRS
マルチプレクサ
M
R
48
50
42
制御回路
40
制御信号入力回路
44
クロックバッファ
46
アドレスバッファ
/CS
/RAS
/CAS
/WE
DQM
CLK
CKE
A0
A10
Am
76
セレクタ
72
レジスタ部
78
80
82
84
86
制御レジスタ
モードレジスタ
ステータスレジスタ
データレジスタ1
データレジスタ2
暗号演算ロジック
74

【図８】

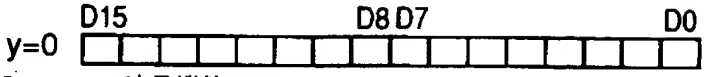

システムメモリマップ
システム予約
外部RAM領域
ROM/Flash領域
ロジック混載DRAM
ロジック制御領域
DRAM領域
制御コマンド領域マップ
予約
データレジスタ2
データレジスタ1
ステータスレジスタ
モードレジスタ
制御レジスタ
X=3FFF,Y=#FF
X=3FFFh,Y=07h～0Ah
X=3FFFh,Y=03h～06h
X=3FFFh,Y=02h
X=3FFFh,Y=01h
X=3FFFh,Y=00h

【図９】



【図１０】

・公開鍵と秘密鍵方式共通

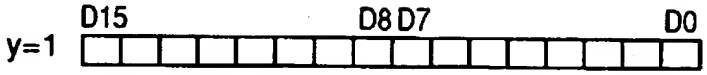


D0　=1:　暗号機能リセット

D1　=1:　暗号処理中を示すフラッグ（0を確認してからアクセスする）

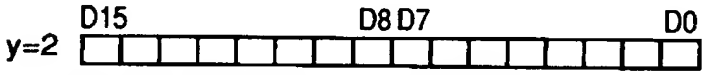
【図１１】

・秘密鍵方式の制御



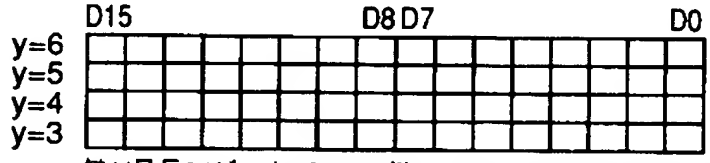
D1,0=01/10/00: DES/Triple DES/ホールド（暗号方式選択、その他は禁止）
D5-2=0001/0010/0100/1000/0000: ECB/CBC/OFB/CFB64/ホールド
（ブロック暗号化モード選択、その他組合せは禁止）
D8-6=001/010/100/000: Normal/Block/Buffer/ホールド
（データ処理モード、その他組合せは禁止）

【図１２】



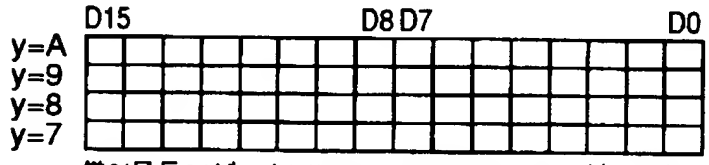
D1,0=01/10/00: 暗号化/復号化/ホールド（11は禁止）
D5,4=01/10/00: 平分または暗号文の入力スタート/ストップ/ホールド（11は禁止）
D9-6=1000-0001/0000: OFB,CFBの1ブロック中のテキスト長(バイト単位)/ホールド
（その他組合せは禁止）

【図１３】



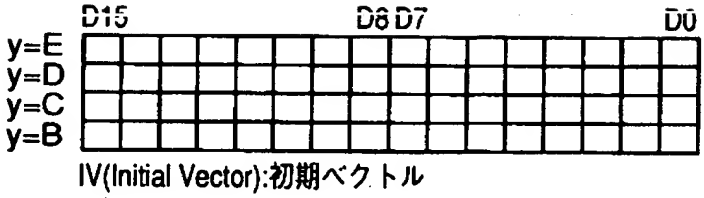
鍵1(最長64ビット):DESの鍵、Triple DESのEDEのEに対する鍵

【図１４】



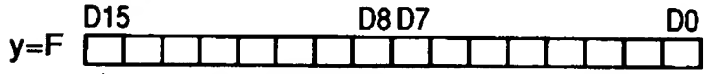
鍵2(最長64ビット):Triple DESのEDEのDに対する鍵

【図１５】



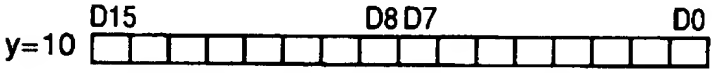
IV(Initial Vector):初期ベクトル

【図１６】



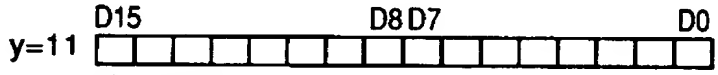
ブロック長:Byte単位で設定　Max=2kByte(D=#FF) Min=1Byte(D=#0)

【図１７】



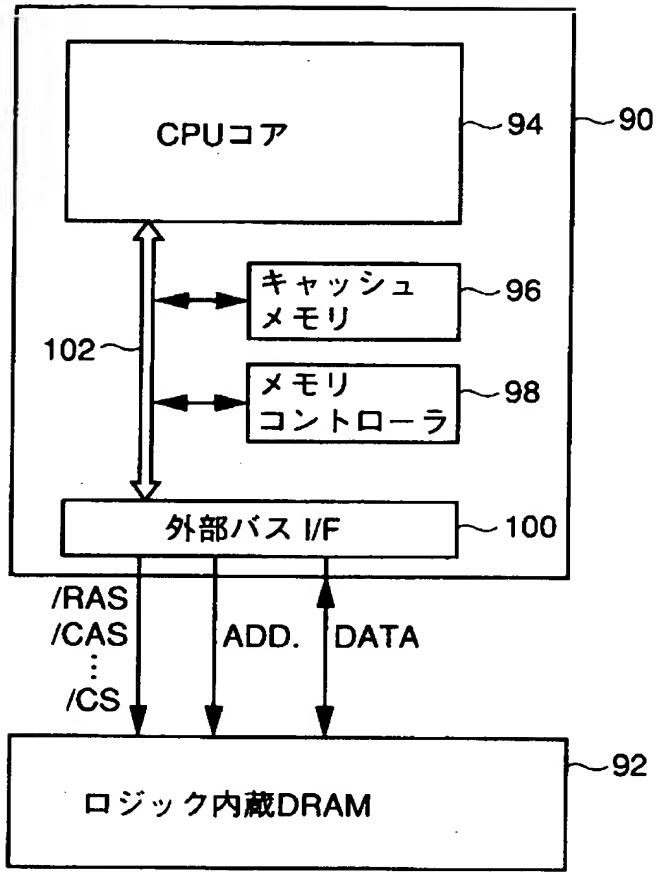
バッファ本数:バッファモードで有効　Max=64k(D=#FFFF) Min=1(D=#0)

【図１８】

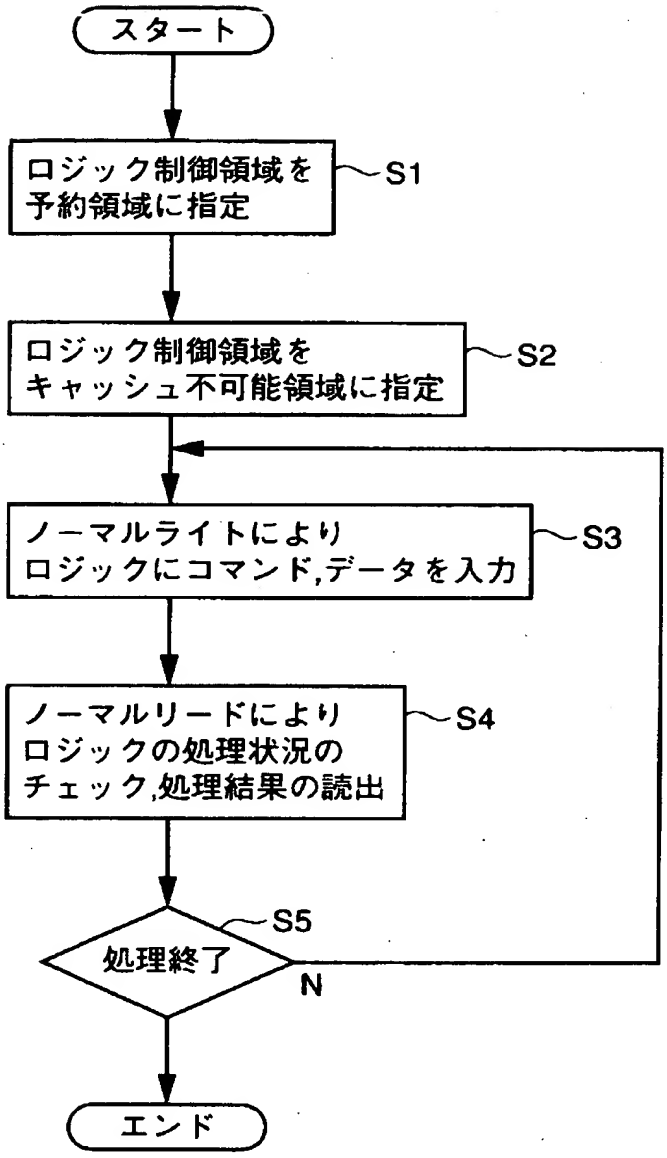


バッファID:

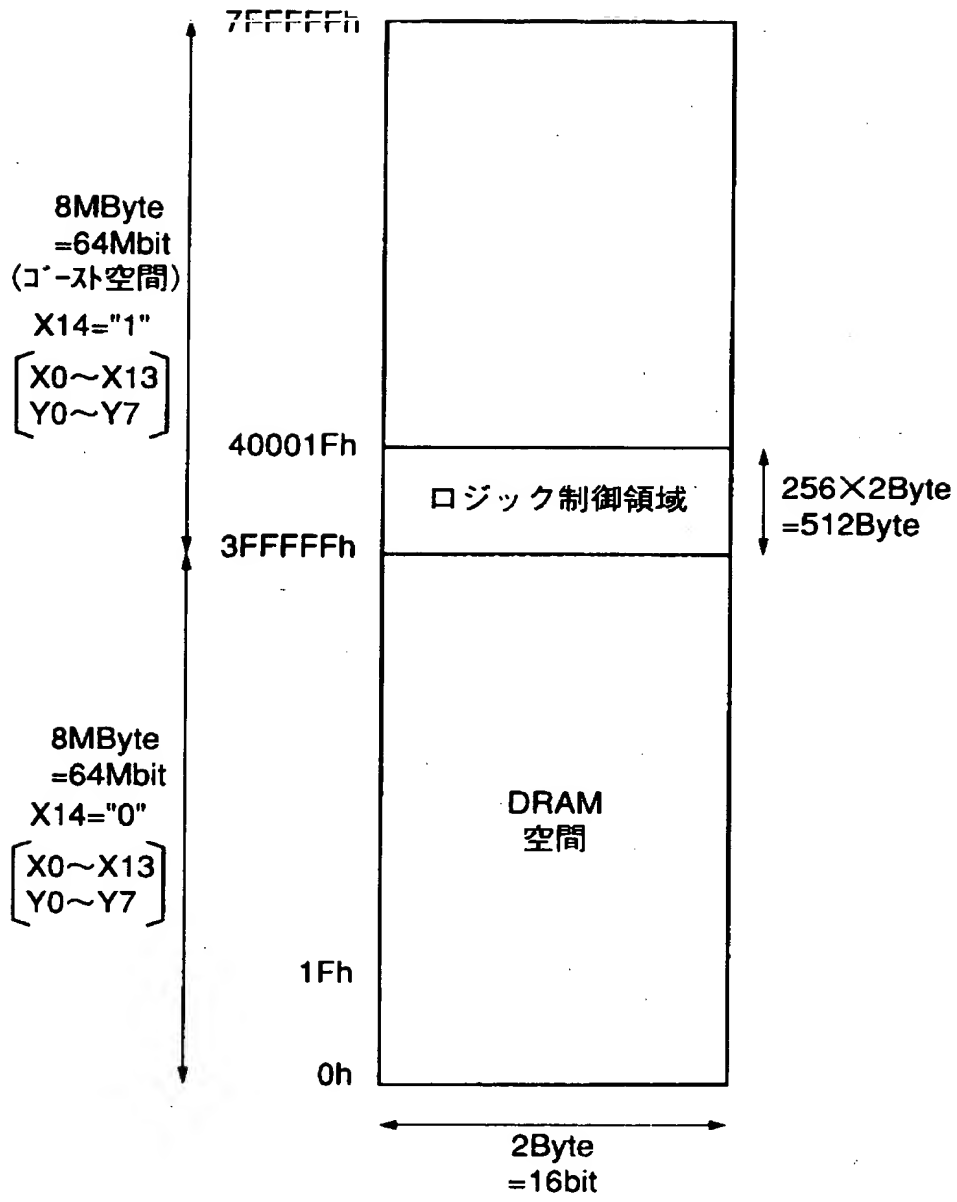
【図１９】


CPUコア
94
90
キャッシュ
メモリ
96
102
メモリ
コントローラ
98
外部バス I/F
100
/RAS
/CAS
/CS
ADD.
DATA
92
ロジック内蔵DRAM

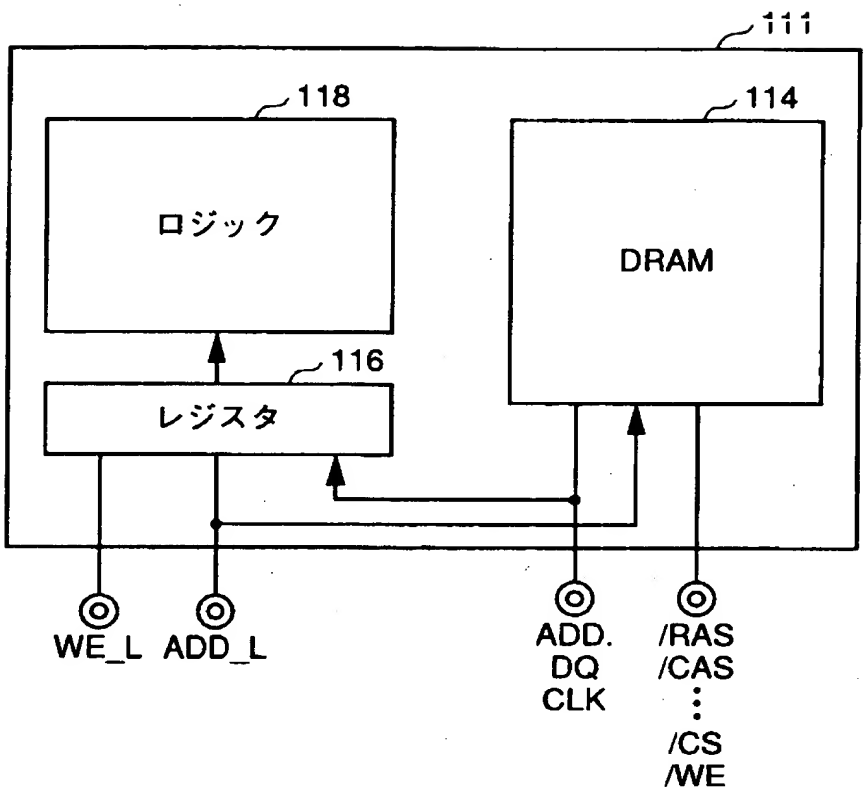
【図２０】


スタート
ロジック制御領域を
予約領域に指定
S1
ロジック制御領域を
キャッシュ不可能領域に指定
S2
ノーマルライトにより
ロジックにコマンド,データを入力
S3
ノーマルリードにより
ロジックの処理状況の
チェック,処理結果の読出
S4
S5
処理終了
N
エンド

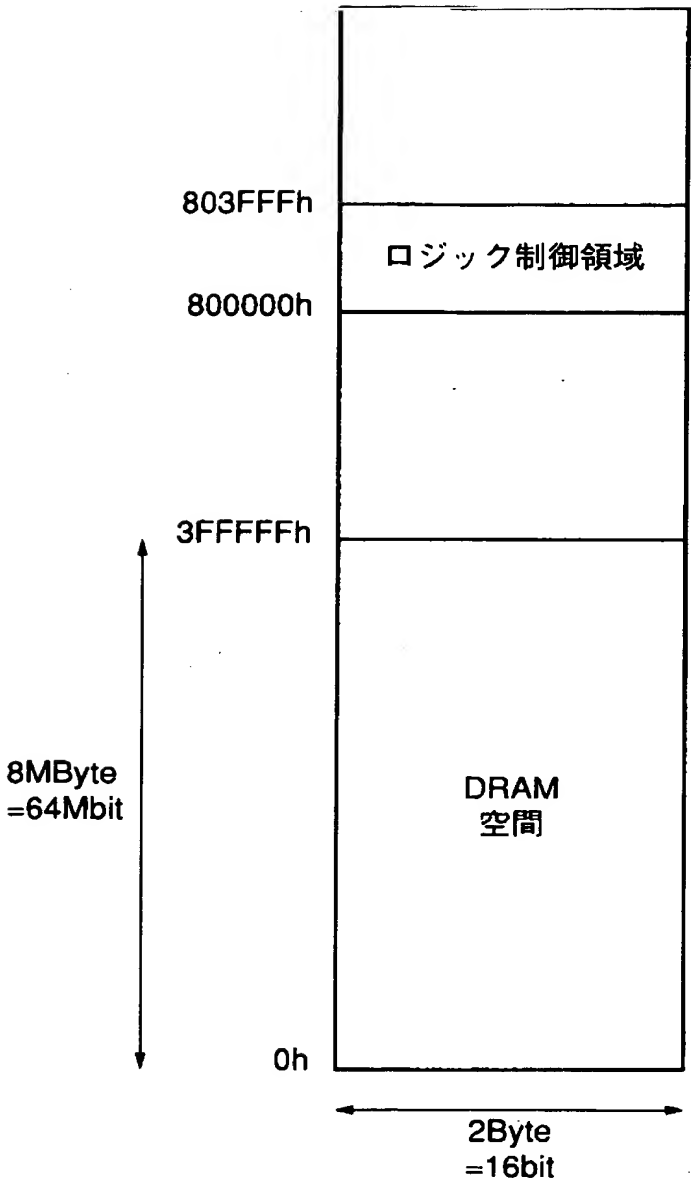
【図２１】


7FFFFFh
8MByte
=64Mbit
(ｺﾞｰｽﾄ空間)
X14="1"
X0～X13
Y0～Y7
40001Fh
ロジック制御領域
256×2Byte
=512Byte
3FFFFFh
8MByte
=64Mbit
X14="0"
X0～X13
Y0～Y7
DRAM
空間
1Fh
0h
2Byte
=16bit

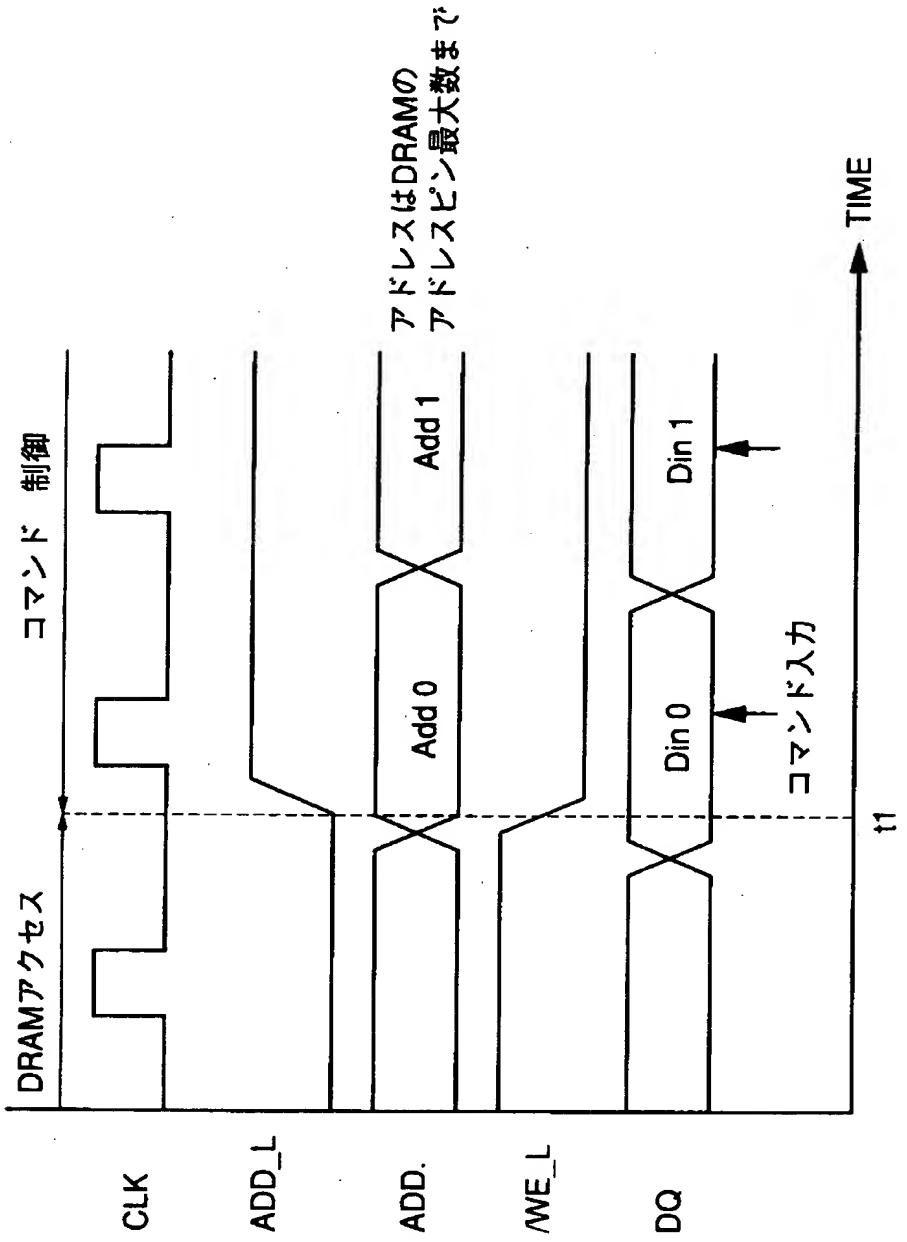
【図２２】



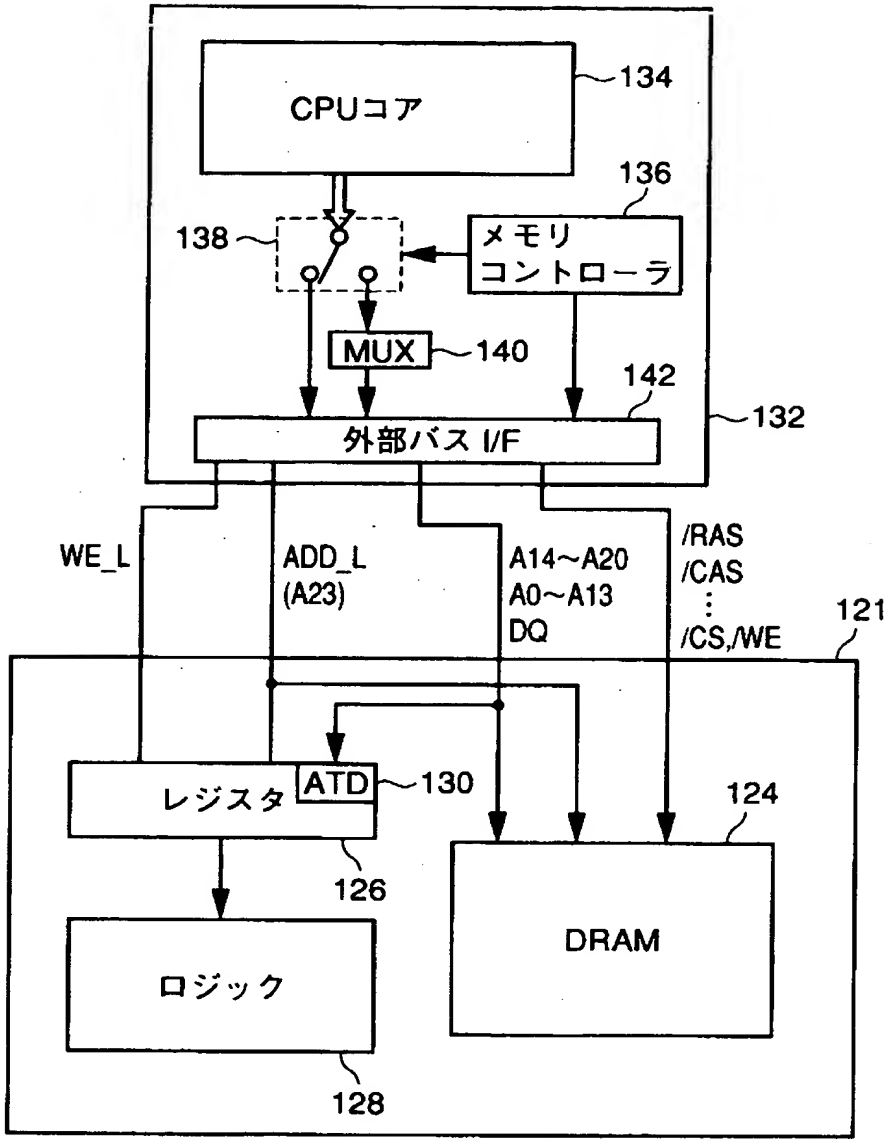
【図２３】


803FFFh
ロジック制御領域
800000h
3FFFFFh
8MByte
=64Mbit
DRAM
空間
0h
2Byte
=16bit

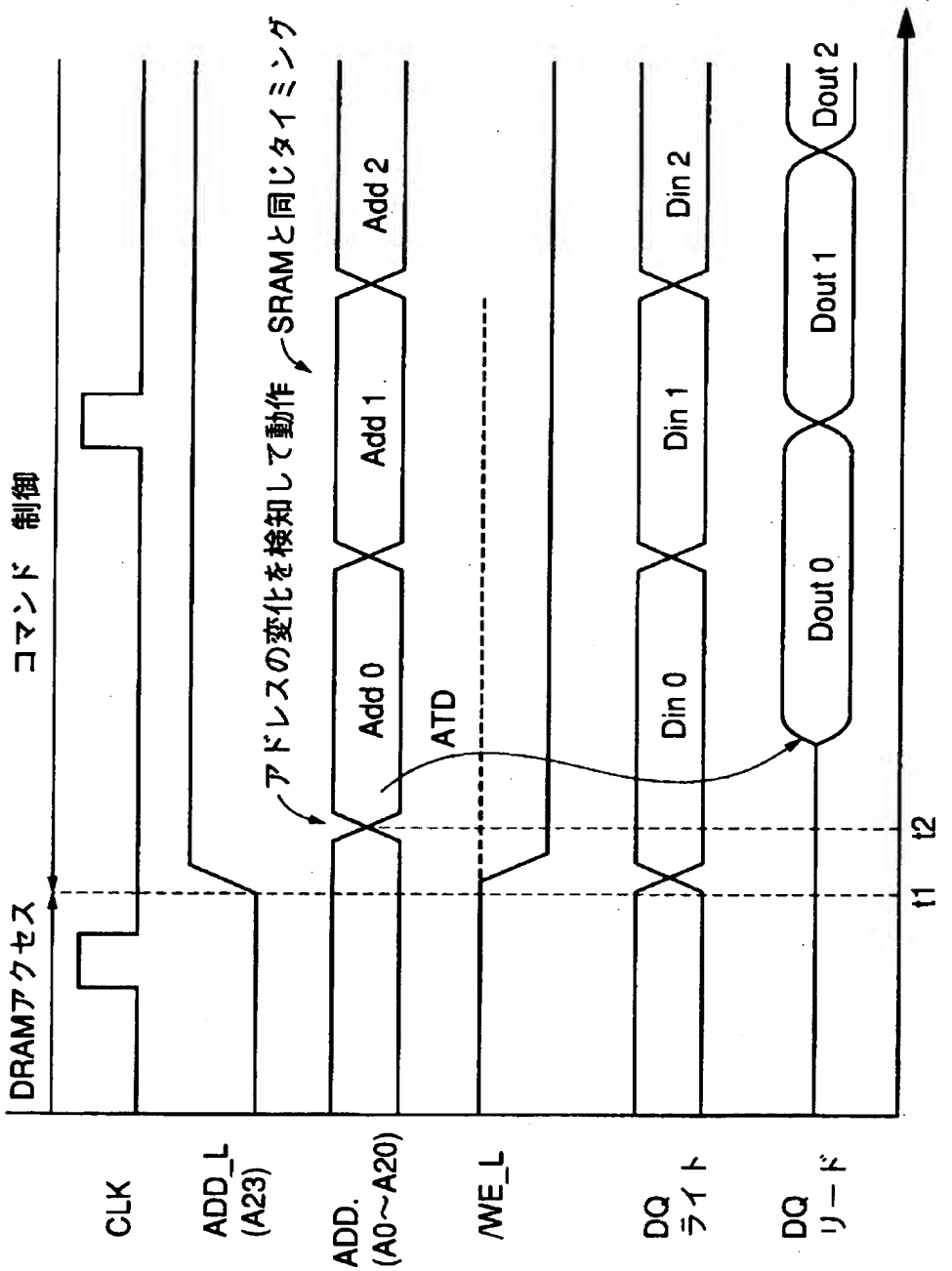
【図２４】


DRAMアクセス
コマンド　制御
アドレスはDRAMの
アドレスピン最大数まで
Add 0
Add 1
Din 0
Din 1
コマンド入力
t1
TIME
CLK
ADD_L
ADD.
/WE_L
DQ

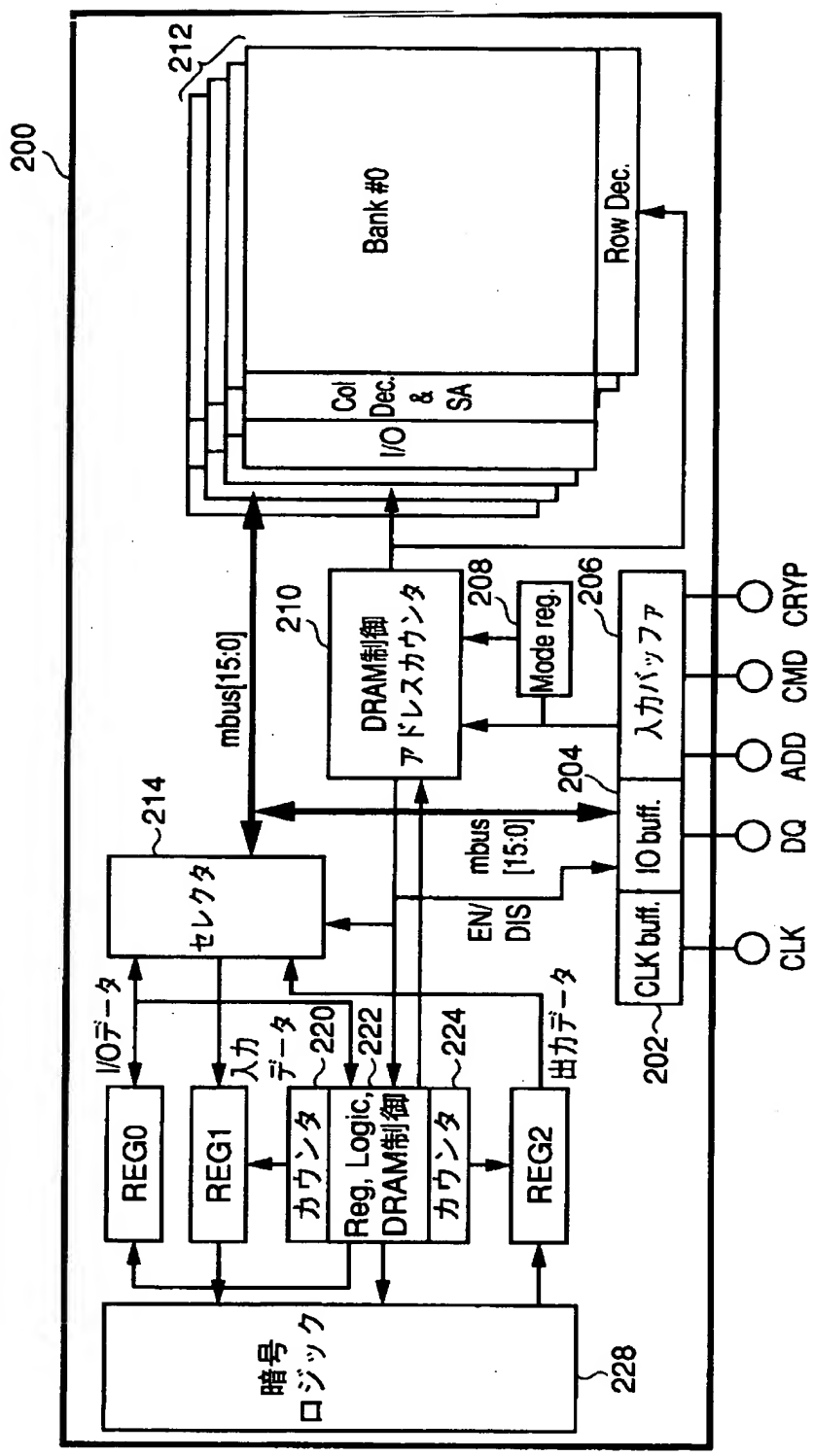
【図２５】


CPUコア
134
136
メモリ
コントローラ
138
MUX
140
142
外部バス I/F
132
WE_L
ADD_L
(A23)
A14～A20
A0～A13
DQ
/RAS
/CAS
/CS,/WE
121
レジスタ
ATD
130
124
126
DRAM
ロジック
128

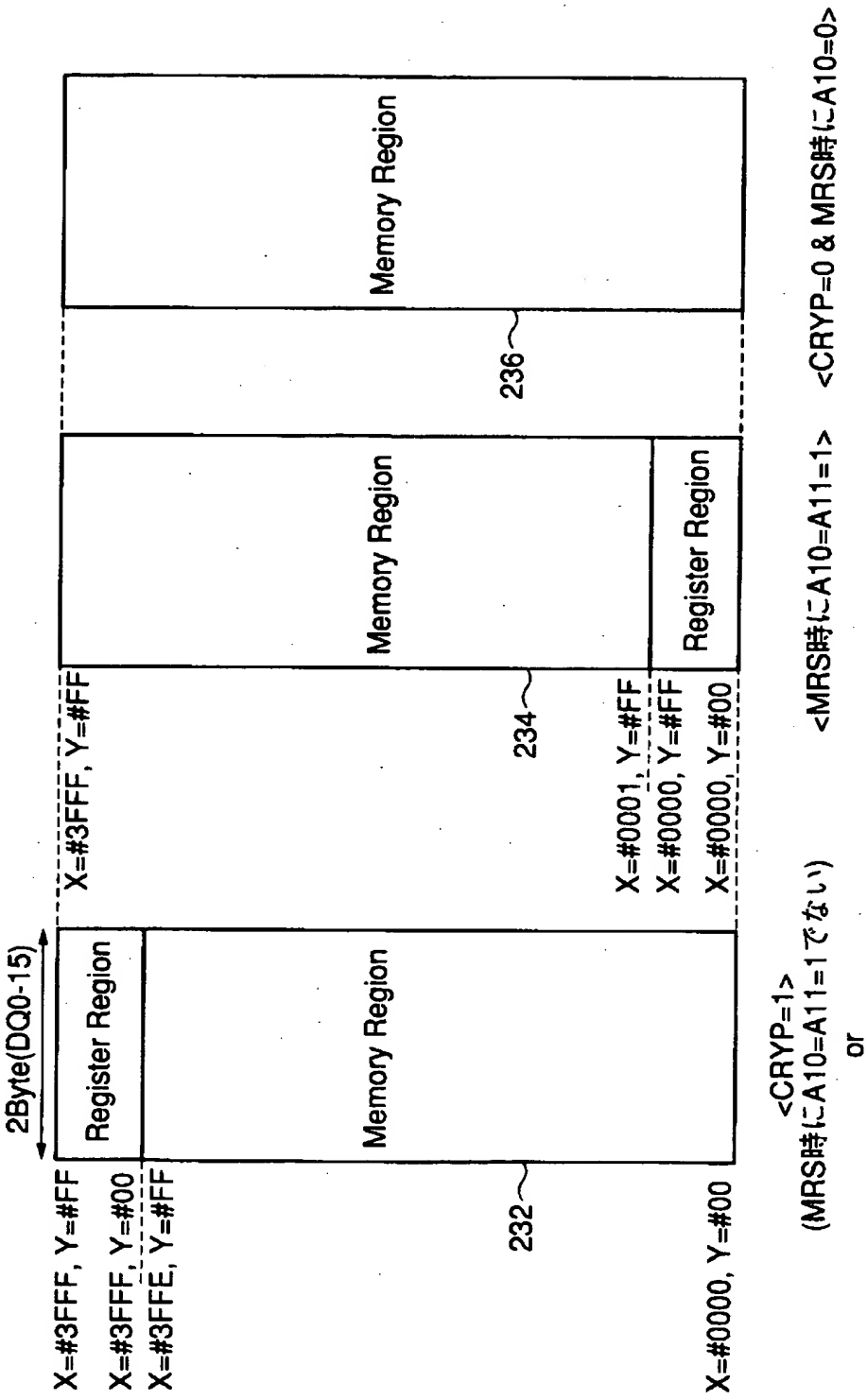
【図２６】


DRAMアクセス
コマンド　制御
アドレスの変化を検知して動作
SRAMと同じタイミング
CLK
ADD_L (A23)
ADD. (A0~A20)
/WE_L
DQ ライト
DQ リード
Add 0
Add 1
Add 2
ATD
Din 0
Din 1
Din 2
Dout 0
Dout 1
Dout 2
t1
t2

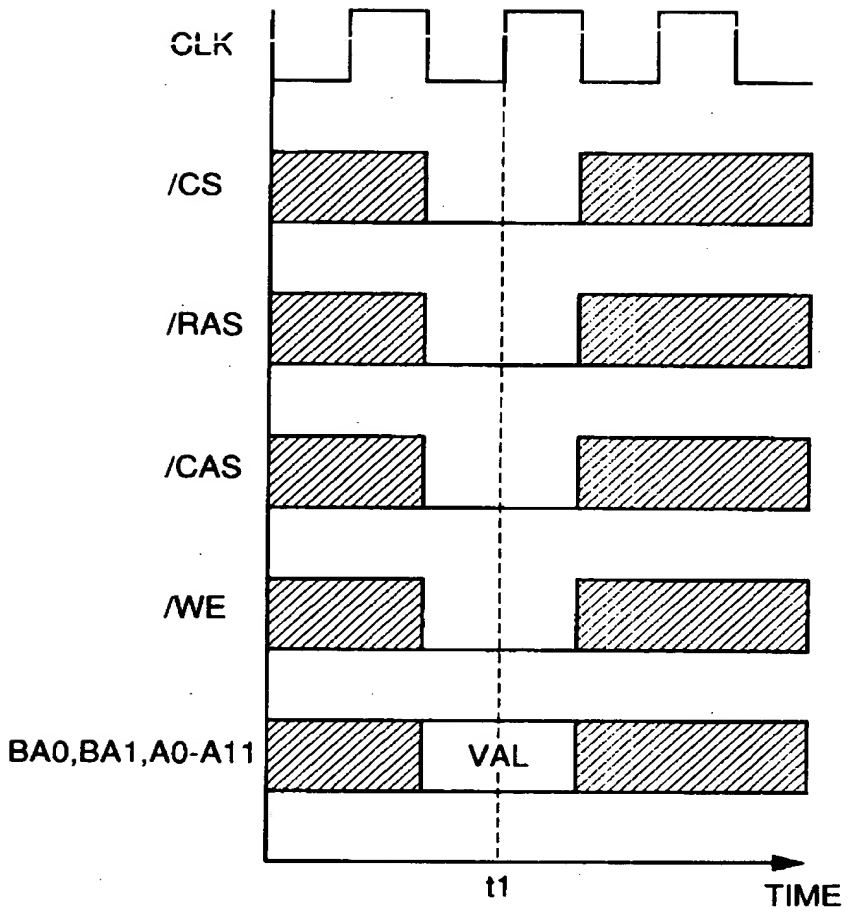
【図２７】


200
212
Bank #0
Row Dec.
Col I/O Dec. & SA
mbus[15:0]
210
DRAM制御 アドレスカウンタ
208
Mode reg.
206
入力バッファ
CRYP
CMD
ADD
DQ
CLK
204
IO buff.
CLK buff.
202
214
セレクタ
mbus [15:0]
EN/ DIS
I/Oデータ
入力データ
220
222
224
出力データ
REG0
REG1
カウンタ
Reg, Logic, DRAM制御
カウンタ
REG2
暗号ロジック
228

【図２８】


2Byte(DQ0-15)
X=#3FFF, Y=#FF
X=#3FFF, Y=#00
X=#3FFE, Y=#FF
X=#0000, Y=#00
X=#3FFF, Y=#FF
X=#0001, Y=#FF
X=#0000, Y=#FF
X=#0000, Y=#00
Register Region
Memory Region
Memory Region
Register Region
Memory Region
232
234
236
<CRYP=1>
(MRS時にA10=A11=1でない)
or
<MRS時にA10=1, A11=0>
<MRS時にA10=A11=1>
<CRYP=0 & MRS時にA10=0>
メモリマップの概略図

【図２９】



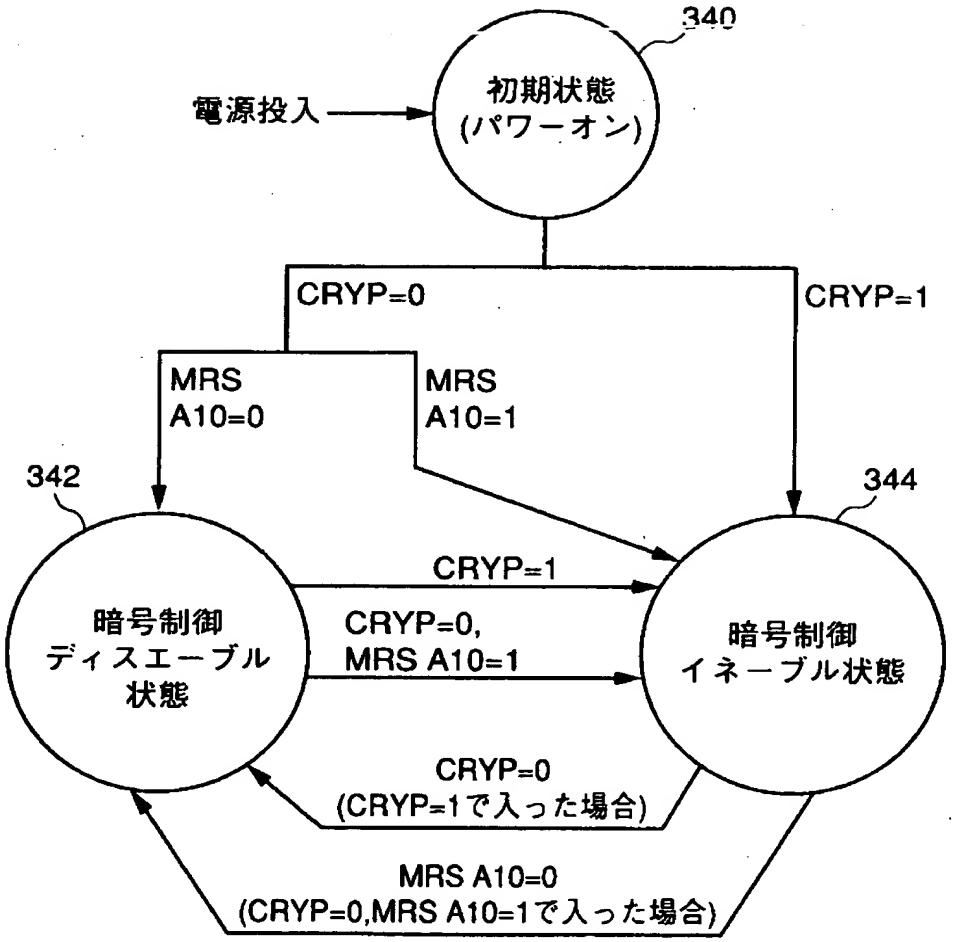
【図３０】

BA0	BA1	A11	A10	A9	A8	A7	A6	A5	A4	A3	A2	A1	A0
					0	0							

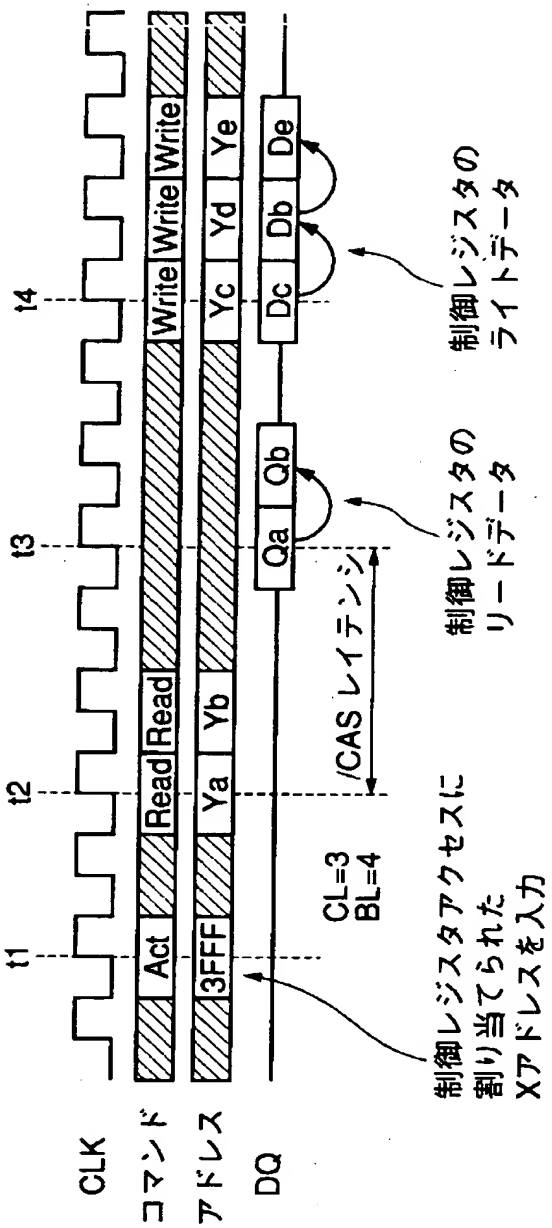
【図３１】

Bits	Name	Description	
A2..0	Burst Length	000 001 010 011 100 101 110 111	1 2 4 8 R R R Full Page
A3	Burst Type	0 1	Sequential Interleaved
A6..4	CAS Latency	000 001 010 011 1XX	R R 2 3 R
A9	Write Mode	0 1	Burst Single Bit
A10	Control Reg. Access	0 1	Disable Enable
A11	Control Reg. Address	0 1	X=3FFF X=0
BA1	Low Power Mode	0 1	Disable Enable
BA0	Low Clock Frequency	0 1	Disable Enable

【図３２】


340
初期状態
(パワーオン)
電源投入
CRYP=0
CRYP=1
MRS
A10=0
MRS
A10=1
342
344
暗号制御
ディスエーブル
状態
CRYP=1
CRYP=0,
MRS A10=1
暗号制御
イネーブル状態
CRYP=0
(CRYP=1で入った場合)
MRS A10=0
(CRYP=0,MRS A10=1で入った場合)

【図３３】


CLK
コマンド
アドレス
DQ
t1
t2
t3
t4
Act
3FFF
Read
Read
Write
Write
Write
Write
Ya
Yb
Yc
Yd
Ye
Qa
Qb
Dc
Db
De
CL=3
BL=4
/CAS レイテンシ
制御レジスタアクセスに
割り当てられた
Xアドレスを入力
制御レジスタの
リードデータ
制御レジスタの
ライトデータ

【図３４】

Col. Add.	Bits	Name	Description		Access
h00	D0	Software Reset	1	Reset	W
	D1	Flag	0	Done	R
			1	Processing	R
	D2	Change add for reg. cont.	1	X=h3FFF	W
	D3	Change add for reg. cont.	1	X=h0	W
	D4	EOF(End of File)	1		W
h01	D1	Partial Refresh	1/0	Bank0 Enable/Disable	W
	D2		1/0	Bank1 Enable/Disable	W
	D3		1/0	Bank2 Enable/Disable	W
	D4		1/0	Bank3 Enable/Disable	W
	D5	LP Mode	1/0	Enable/Disable	W
	D6	Low Clock Frequency	1/0	Enable/Disable	W

【図３５】

Col. Add.	Bits	Name	Description		Access
h02	D1..0	Secret Cryp. Mode	00	Hold	W
			01	DES-56	W
			10	Triple DES-112	W
			11	Triple DES-168	W
	D5..2	Block Cryp. Mode	0000	Hold	W
			0001	ECB	W
			0010	CBC	W
			0100	OFB	W
			1000	CFB-64	W
	D9..6	Enabled bank set in Reg-DRAM transfer mode	0000	All Bank Disable	W
	D6		1/0	Bank0 Enable/Disable	W
	D7		1/0	Bank1 Enable/Disable	W
	D8		1/0	Bank2 Enable/Disable	W
	D9		1/0	Bank3 Enable/Disable	W
	D10	Simulatenous transfer	1/0	Enable/Disable	W

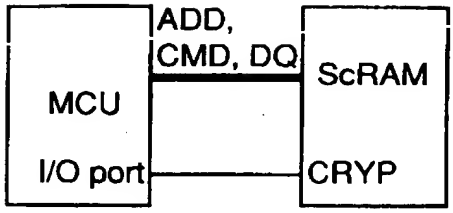
【図３６】

Col. Add.	Bits	Name	Description		Access
h03	D1..0	ENC/DEC	00	Hold	W
			01	Encryption	W
			10	Decryption	W
			11	RFU	W
	D2	Counter of reg1	1	Reset	W
	D3	Counter of reg2	1	Reset	W
	D4	IV Load	0	Previous output	W
			1	IV Load	W
	D8..5	Text length per block	0000	Hold	W
			Else	(D8..5)x1Byte	W
h04	D15..0	Reg.1 Access	-	Write Data: D15..0	W
h05	D15..0	Reg.2 Access	-	Read Data: D15..0	R
h06	D0	Reg-DRAM transfer	1	Mode entry Mode exit	W
	D1		1		W
	D2		1	Counter reset of reg1	W
	D3		1	Counter reset of reg1	W

【図３７】

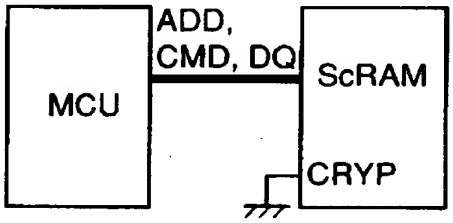
Col. Add.	Bits	Name	Description		Access
h13-h10	D15..0	Key1 for DES, Triple DES	LSB: h10[D0] USB: h13[D15]	Key1 Input	W
h17-h14	D15..0	Key2 for Triple DES	LSB: h14[D0] USB: h17[D15]	Key2 Input	W
h1B-h18	D15..0	Key3 for Triple DES-168	LSB: h18[D0] USB: h17B[D15]	Key3 Input	W
h1F-h1C	D15..0	Initial Vector (IV)	LSB: h1C[D0] USB: h1F[D15]	IV Input	W
hFF-h20	D15..0	Reserved			

【図３８】



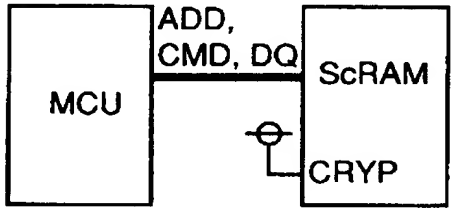
CRYP端子をI/O portで制御

【図３９】



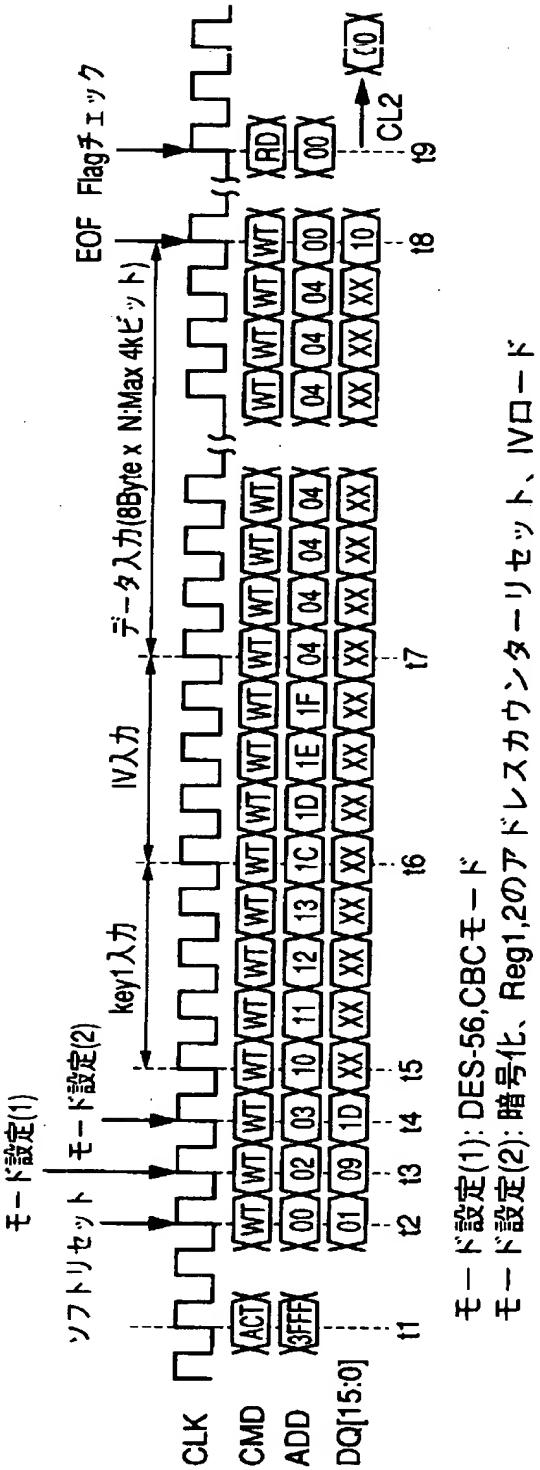
CRYP端子をL固定

【図４０】

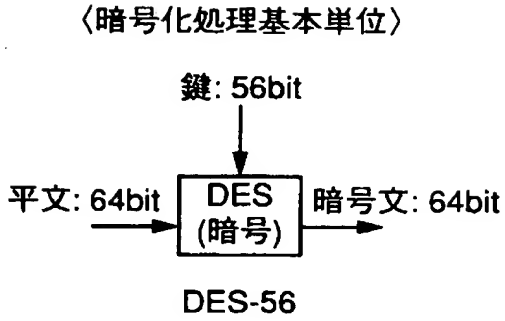


CRYP端子をH固定

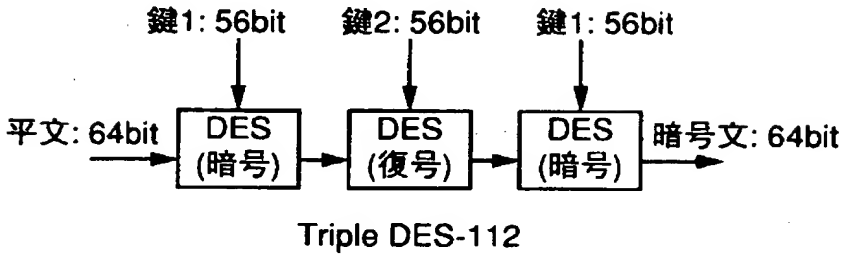
【図４１】


ソフトリセット
モード設定(1)
モード設定(2)
key1入力
IV入力
データ入力(8Byte x N:Max 4kビット)
EOF Flagチェック
CL2
CLK
CMD
ADD
DQ[15:0]
ACT
3FFF
WT
00
01
02
09
03
1D
10
XX
11
12
13
1C
1D
1E
1F
04
RD
t1
t2
t3
t4
t5
t6
t7
t8
t9
モード設定(1): DES-56,CBCモード
モード設定(2): 暗号化、Reg1,2のアドレスカウンターリセット、IVロード

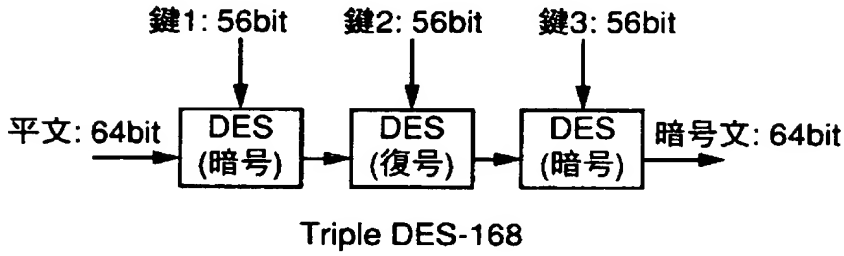
【図４２】


〈暗号化処理基本単位〉
鍵: 56bit
平文: 64bit
DES
(暗号)
暗号文: 64bit
DES-56

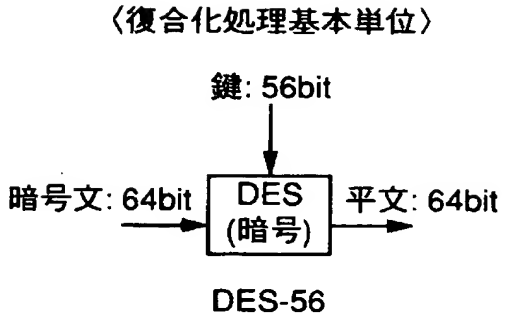
【図４３】


鍵1: 56bit
鍵2: 56bit
鍵1: 56bit
平文: 64bit
DES
(暗号)
DES
(復号)
DES
(暗号)
暗号文: 64bit
Triple DES-112

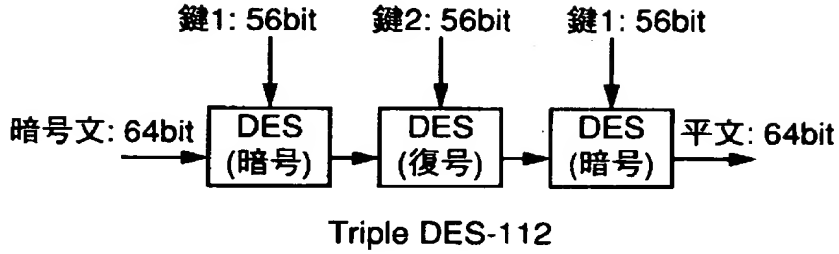
【図４４】


鍵1: 56bit
鍵2: 56bit
鍵3: 56bit
平文: 64bit
DES
(暗号)
DES
(復号)
DES
(暗号)
暗号文: 64bit
Triple DES-168

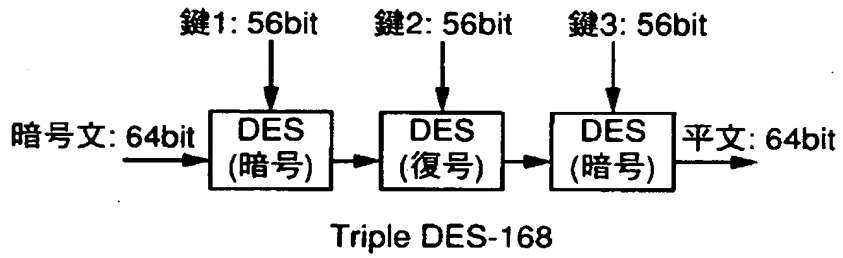
【図４５】



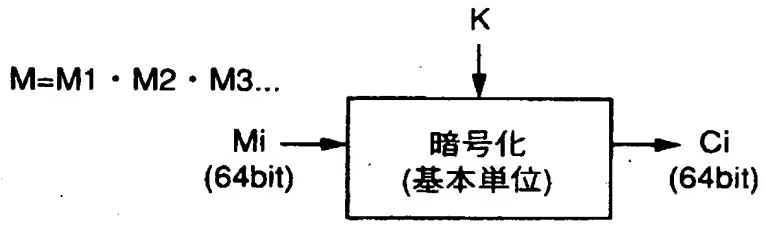
【図４６】



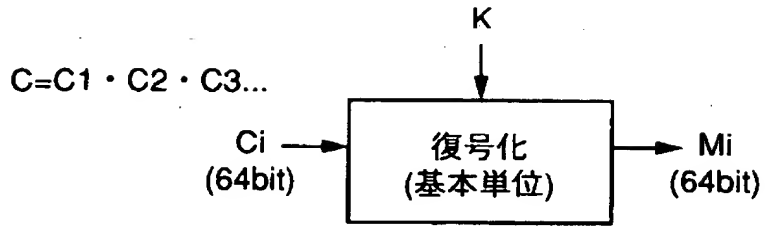
【図４７】



【図４８】



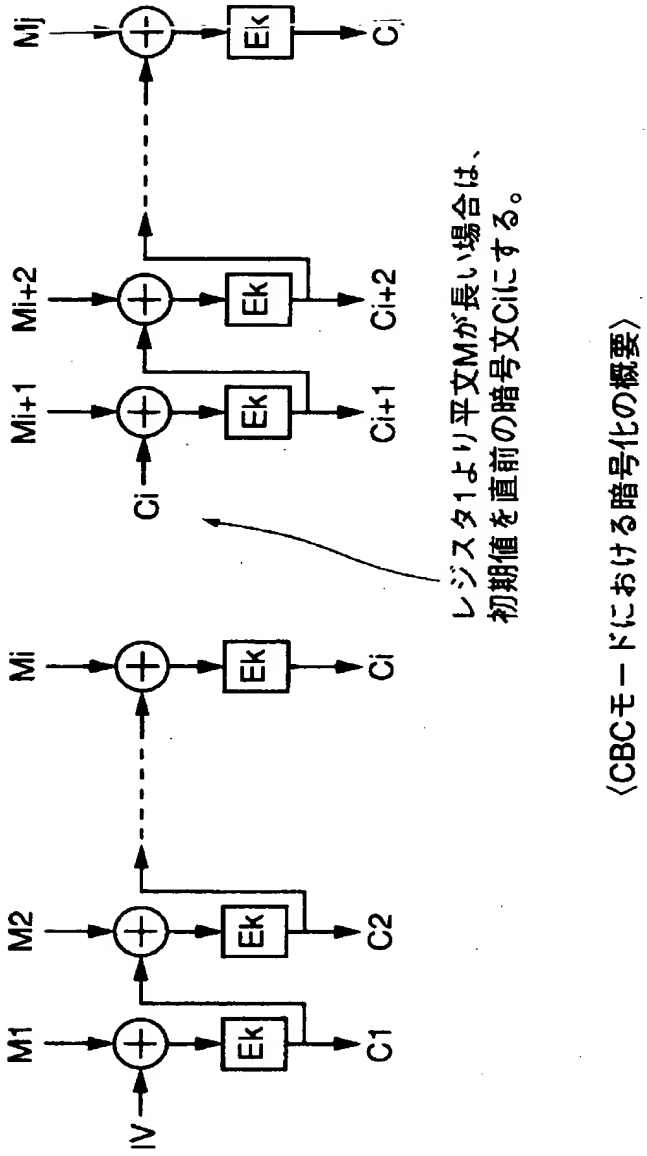
【図４９】



【図５０】

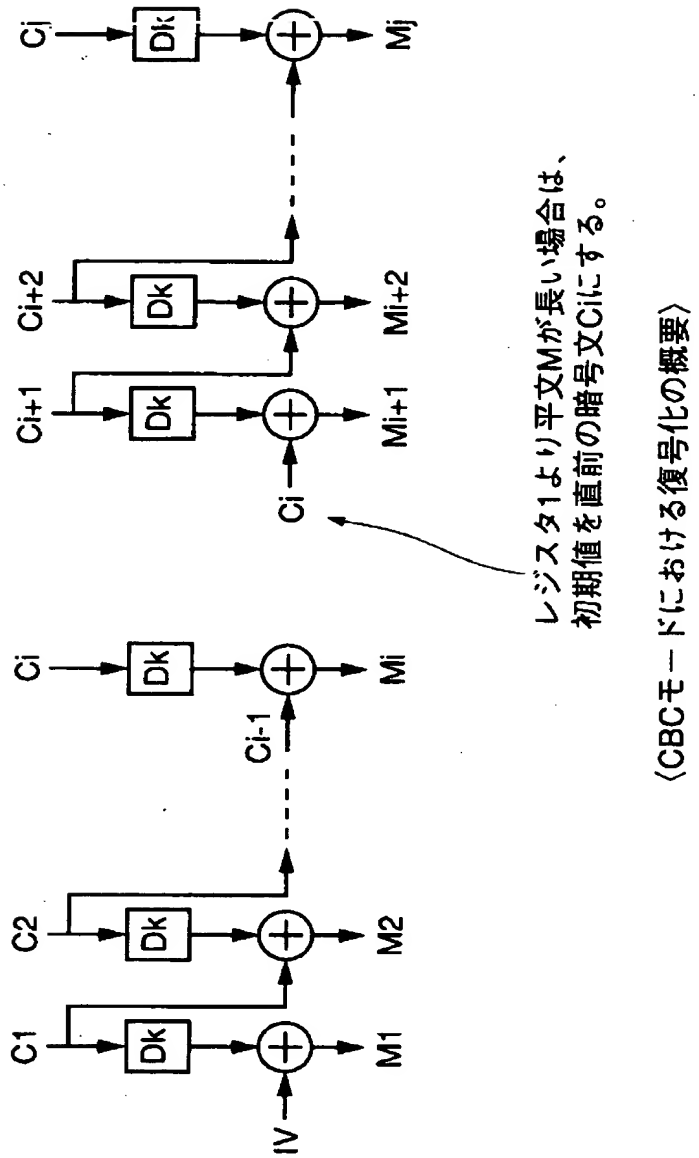
C1=Ek (M1 ⊕ IV)
Ci=Ek (Mi ⊕ Ci-1) (i=2,3,.....)
M1=Dk (C1) ⊕ M1
Mi=Dk (Ci) ⊕ Ci-1 (i=2,3,.....)

【図５１】

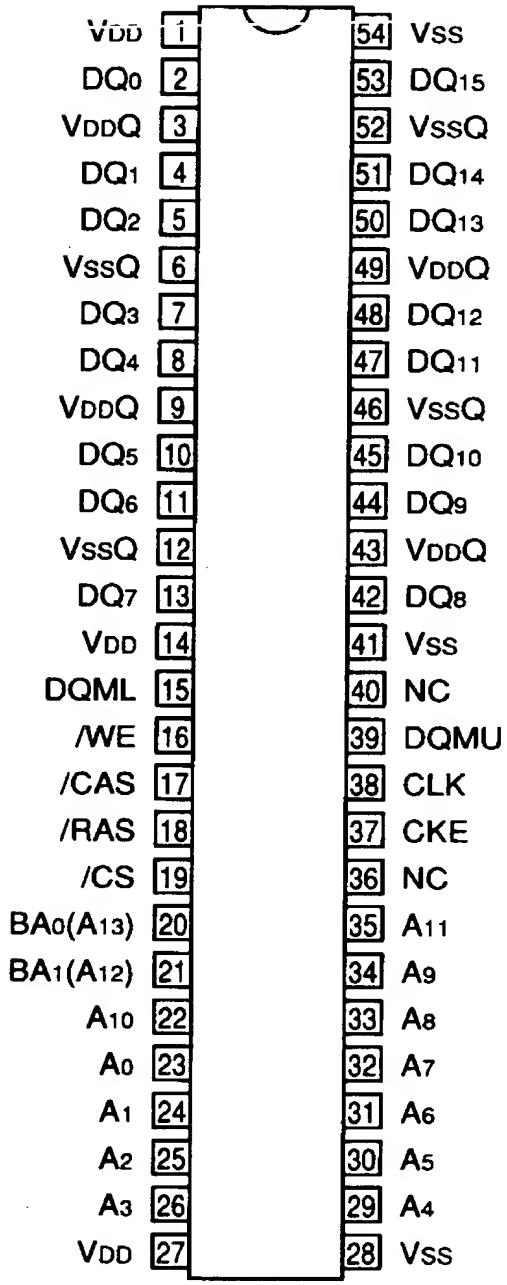


〈CBCモードにおける暗号化の概要〉

【図５２】


Cj
Dk
Mj
Ci+2
Mi+2
Ci+1
Mi+1
Ci
Mi
Ci-1
C2
M2
C1
M1
IV
レジスタ1より平文Mが長い場合は、
初期値を直前の暗号文Ciにする。
〈CBCモードにおける復号化の概要〉

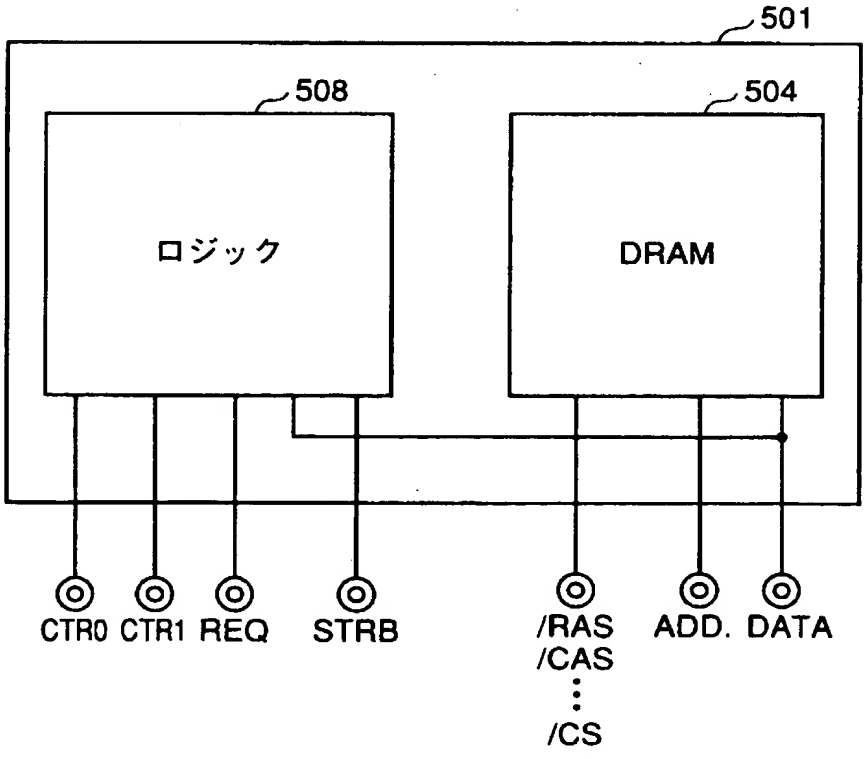
【図５３】


VDD 1
DQ0 2
VDDQ 3
DQ1 4
DQ2 5
VSSQ 6
DQ3 7
DQ4 8
VDDQ 9
DQ5 10
DQ6 11
VSSQ 12
DQ7 13
VDD 14
DQML 15
/WE 16
/CAS 17
/RAS 18
/CS 19
BA0(A13) 20
BA1(A12) 21
A10 22
A0 23
A1 24
A2 25
A3 26
VDD 27
54 VSS
53 DQ15
52 VSSQ
51 DQ14
50 DQ13
49 VDDQ
48 DQ12
47 DQ11
46 VSSQ
45 DQ10
44 DQ9
43 VDDQ
42 DQ8
41 VSS
40 NC
39 DQMU
38 CLK
37 CKE
36 NC
35 A11
34 A9
33 A8
32 A7
31 A6
30 A5
29 A4
28 VSS

【図５４】

端子名	機能
CLK	マスタクロック
CKE	クロックイネーブル
/CS	チップセレクト
/RAS	行アドレスストローブ
/CAS	列アドレスストローブ
/WE	ライトイネーブル
$DQ_{0\sim15}$	データ入出力
DQM(U/L)	出力ディスエーブル/ライトマスク
$A_{0\sim11}$	アドレス入力
$BA_{0,1}(A_{12,13})$	バンクアドレス
V_{DD}	電源
$V_{DD}Q$	出力用電源
V_{SS}	接地
$V_{SS}Q$	出力用接地

【図５５】



【書類名】　　要約書

【要約】

【課題】　マイコンシステムにおいて制御しやすいロジック内蔵ＤＲＡＭを提供する。

【解決手段】　インタフェース部２は、アドレス信号ＡＤＤ．で指定される領域が、ロジック制御領域である場合には、ＤＲＡＭ４とデータを授受する代わりに、レジスタ６とデータ授受を行なう。その際のデータ信号ＤＡＴＡは、レジスタ６に保持されるロジック回路８に対する制御コマンドや、処理のための入力データである。レジスタ６の保持内容に応じて、ロジック回路８は、たとえば、暗号処理や、画像処理等の、マイコンでは時間を要してしまう処理を実行する。処理結果はレジスタ６に保存され、ＤＲＡＭに対する読出と同様のシーケンスで読出される。

【選択図】　　図１

出願人履歴情報

識別番号　〔０００００６０１３〕

１．変更年月日　１９９０年　８月２４日
［変更理由］　新規登録
住　所　東京都千代田区丸の内２丁目２番３号
氏　名　三菱電機株式会社